McAfee Change Control and Application Control 6.0.0 Product Guide

For use with ePolicy Orchestrator 4.5.0 and 4.6.0

Contents

Introduction

Get familiar with the McAfee® Change Control® and McAfee® Application Control® software and learn how they protect your environment.

Contents

McAfee Change Control overview

Change Control allows you to monitor and prevent changes to the file system, registry, and user accounts. You can view details of who made changes, which files were changed, what changes were made to the files, and when and how the changes were made. You can write-protect critical files and registry keys from unauthorized tampering. You can read-protect sensitive files. To ease maintenance, you can define trusted programs or users to allow updates to protected files and registry keys.

In effect, a change is permitted only if the change is applied in accordance with the update policies. Using Change Control, you can:

- Detect, track, and validate changes in real-time
- Gain visibility into ad-hoc changes
- Eliminate ad-hoc changes using protection rules
- Enforce approved change policies and compliance

Real-time monitoring

Change Control provides real-time monitoring for file and registry changes. Real-time monitoring eliminates the need to perform scan after scan on endpoints and identifies transient change violations, such as when a file is changed and restored to its earlier state. It captures every change, including the time of the change, who made the change, what program was used to make the change, and whether the change was made manually or by an authorized program. It maintains a comprehensive and up-to-date database (on McAfee® ePolicy Orchestrator®) that logs all attempts to modify files, registry keys, and local user accounts.

Customizable filters

You can use filters to ensure that only relevant changes make it to the database. You can define filters to match the file name, directory name, registry key, process name, file extension, and user name. Using the criteria, you can define two types of filters:

- Include filters to receive information on events matching the specified filtering criteria.
- Exclude filters to ignore information on events matching the specified filtering criteria.

Filtering events is needed to control the volume of change events. Typically, a number of changes are program-generated and need not be reported to the system administrator. If programmatic and automatic change activity is high, a large number of change events can overwhelm the system. Using filters ensures that only relevant change events are recorded.

Read protection

Read-protection rules prevent users from reading the content of specified files, directories, and volumes. If a directory or volume is read-protected, all files in the directory or volume are read-protected. Once defined, read-protection rules are inherited by subdirectories. You cannot read-protect registry keys.

NOTE: By default, read protection is disabled.

Write protection

Use write-protection rules to prevent users from creating new files (including directories and registry keys) and modifying existing files, directories, and registry keys. Write-protecting a file or registry key renders it read-only and protects it from unanticipated updates. The following actions are prevented for a write-protected file or registry key:

- Delete
- Rename
- Create hard links
- Modify contents
- Append
- Truncate
- Change owner
- Create Alternate Data Stream (Microsoft Windows only)

McAfee Application Control overview

Today's IT departments face tremendous pressure to ensure that their endpoints comply with many different security policies, operating procedures, corporate IT standards, and regulations. Extending the viability of fixed function devices such as point-of-sale (POS) terminals, customer service terminals, and legacy NT platforms has become critical.

Application Control uses dynamic whitelisting to ensure that only trusted applications run on devices, servers and desktops. This provides IT with the greatest degree of visibility and control over clients, and helps enforce software license compliance. Here are some product features.

- Protects your organization against malware attacks before they occur by proactively controlling the applications executing on your desktops, laptops, and servers.
- Locks down the protected endpoints against threats and unwanted changes, with no file system scanning or other periodic activity that could impact system performance.
- Augments traditional security solutions and enables IT to allow only approved system and application software to run. Blocks unauthorized or vulnerable applications that may compromise endpoints without imposing operational overhead. This ensures that end-users cannot accidentally introduce software that poses a risk to the business.

- Uses dynamic whitelisting to ensure that only trusted applications run on devices, servers, and desktops. McAfee's dynamic whitelisting trust model eliminates the labor and cost associated with other whitelisting technologies, thereby reducing overhead and increasing continuity.
- Provides IT control over endpoints and helps enforce software license compliance. With McAfee Application Control, IT departments can eliminate unauthorized software on endpoints, while providing employees greater flexibility to use the resources they need to get their jobs done.
- Eliminates the need for IT administrators to manually maintain lists of approved applications. This enables IT departments to adopt a flexible approach where a repository of trusted applications can run on endpoints. This prevents execution of all unauthorized software scripts and dynamic link libraries (DLLs), and further defends against memory exploits.
- Works effectively when integrated with McAfee ePO and in standalone mode without network access. The product is designed to operate in a variety of network and firewall configurations.
- Runs transparently on endpoints. It can be set up quickly with very low initial and ongoing operational overhead and minimal impact on CPU cycles.

About this guide

This guide describes how to configure and use Change Control and Application Control with McAfee ePO versions 4.6 or 4.5.

Prerequisites

Before you can configure and use Change Control or Application Control, you must:

- Ensure that McAfee ePO 4.6 or 4.5 is installed and running. For more information on installing McAfee ePO 4.6 or 4.5, refer to the *ePolicy Orchestrator 4.6 Installation Guide* or *ePolicy Orchestrator 4.5 Installation Guide*, respectively.
- Ensure that Change Control or Application Control is installed and running. For more information on installation, refer to the *McAfee Change Control and Application Control Installation Guide*.
- Ensure valid licenses are added for using Application Control and Change Control. For more information on adding licenses, refer to the *McAfee Change Control and Application Control Installation Guide*.

Using this guide

This document is meant as a reference to use along with the Change Control, Application Control, and McAfee ePO interfaces. This document provides information on configuring and using the Change Control and Application Control products.

Section	Description	Applies to Change Control	Applies to Application Control
Introduction	Provides an overview of the Change Control and Application Control products.	√	√
Getting started with Change Control	Details the various Change Control-related concepts, such as modes and rule groups and describes how to enable the product.	√	NA

Section	Description	Applies to Change Control	Applies to Application Control
Monitoring the file system and registry	Provides concepts and instructions to help you define rules to monitor files and registry entries for changes.	√	NA
Protecting the file system and registry	Provides concepts and instructions to help you define rules to read-protect and write-protect files and registry entries.	√	NA
Monitoring and reporting	Describes how to use events, dashboards, and queries to monitor the network status when using the Change Control product.	√	NA
Getting started with Application Control	Details the various Application Control-related concepts, such as modes, trust model, rule groups, installers, and publishers.	NA	√
Deploying Application Control in Observe mode	Provides detailed instructions to help you place Application Control in the Observe mode to perform a dry run for the product.	NA	√
Monitoring your protection	Describes how to enable Application Control and details routine tasks to perform when the product is running in Enabled mode.	NA	√
Managing the inventory	Provides instructions to help you fetch, review, and manage the software inventory for protected endpoints.	NA	√
Using dashboards and queries	Describes how use to dashboards and queries to monitor the network status when using the Application Control product.	NA	√
Maintaining your systems	Details various tasks to help you maintain the protected endpoints.	√	√
Fine-tuning your configuration	Describes advanced configuration tasks that help you fine tune your configuration.	√	√
FAQs	Provides answers to frequently asked questions.	√	√

Product documentation

To access the documentation for the Change Control or Application Control products, use the McAfee ServicePortal (http://mysupport.mcafee.com).

1. Navigate to the McAfee ServicePortal.
2. Click **Product Documentation** under **Self Service**.
3. Select the product.
4. Select a version.
5. Select a product document.

NOTE: Click **Search the KnowledgeBase** for answers to your product questions and **Browse the KnowledgeBase** for articles listed by product and version.

Documents available

The following product documents are available (as PDF files) from the McAfee Downloads site (http://www.mcafee.com/us/downloads/downloads.aspx) and McAfee ServicePortal.

- *Installation Guide*: Provides instructions for installing, upgrading, and uninstalling the Change Control and Application Control software.
- *Product Guide*: Introduces the product and provides detailed instructions for configuring and using the product features.
- *Change Control Evaluation Guide*: Provides detailed procedures to implement common file monitoring and change prevention use cases.
- *Application Control Evaluation Guide*: Provides detailed procedures to implement whitelisting use cases.
- *Release Notes*: Highlights new features and details important information for the release.

Getting started with Change Control

Before you begin using Change Control, get familiar with it and understand related concepts.

Contents

Understanding Change Control modes

At any time, Change Control can operate in one of these modes.

Enabled	Indicates that the software is in effect and changes are monitored and controlled on the endpoints as per the defined policies. When in Enabled mode, Change Control monitors and protects files and registry keys as defined by the configured policies. Enabled mode is the recommended mode of operation. From the Enabled mode, you can switch to the Disabled or Update mode.
Update	Indicates that the software is in effect, allows ad-hoc changes to the endpoints, and tracks the changes made to the endpoints. Use the Update mode to perform scheduled or emergency changes, such as software and patch installations. In the Enabled mode, you cannot read the read-protected files or modify any write-protected files (as per the defined policies). However, in the Update mode, all read and write protection that is in effect is overridden. Use the Update mode to define a change window during which you can make changes to endpoints and authorize the made changes. From the Update mode, you can switch to the Enabled or Disabled mode. We recommend that you switch to the Enabled mode as soon as the changes are complete.
Disabled	Indicates that the software is not in effect. Although the software is installed, the associated features are not active. When you place the endpoints in Disabled mode, the application restarts the endpoints. From the Disabled mode, you can switch to the Enabled or Update mode.

Managing rule groups

As the name suggests, a rule group is a collection of rules. Although you can directly add rules to any McAfee ePO-based policy, the rules defined within a policy are specific to that policy. In contrast, a rule group is an independent unit that collates a set of similar or related rules. After you define a rule group, you can reuse the rules within the rule group by associating the rule group with different policies. Also, if you need to modify a rule, simply update the rule in the rule group and the change cascades across all associated policies automatically.

Change Control provides predefined rule groups to monitor commonly-used applications. Although you cannot edit the predefined rule groups, you can use an existing rule group as a starting point to develop your rule groups. You can create a copy of an existing rule group and edit it

to add more rules or create a new rule group. If needed, you can also import or export rule groups.

When do I use rule groups?

If you need to define similar rules across policies, using rule groups can drastically reduce the effort required to define rules. If you have a large setup and are deploying the software across numerous endpoints, we recommend you use rule groups to minimize the deployment time and effort.

Consider an example. An organization runs Oracle on multiple servers. Each of these servers is used by the HR, Engineering, and Finance departments for different purposes. To reduce rule redundancy, we define these rule groups with Oracle-specific rules.

- An Integrity Monitor rule group (named IM-Oracle) containing rules to monitor and track configuration files and registry keys (to help audit critical changes to Oracle configuration)
- A Change Control rule group (named CC-Oracle) containing rules to protect critical files for Oracle (to prevent unauthorized changes)

After the rule groups are defined, we can reuse these rule groups across policies for the HR, Engineering, and Finance departments. So, when defining policies for the *HR Servers*, add the IM-Oracle rule group to a monitoring (Integrity Monitor) policy and CC-Oracle rule group to a protection (Change Control) policy along with rule groups for the other applications installed on the HR server. Similarly, add the IM-Oracle and CC-Oracle rule groups to the relevant policies for the *Engg Servers* and *Fin Servers*. After defining the policies, if you realize that the rule for a critical file was not created, directly update the rule group and all the policies will be updated automatically.

Contents

Creating rule groups

Use this task to create a rule group.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Solidcore Rules**.

2 Perform one of these steps from the **Rule Groups** tab.

- Select **Integrity Monitor** to view or define a rule group for monitoring changes performed on critical resources.
- Select **Change Control** to view or define a rule group for preventing unauthorized changes on critical resources.

You can use an existing rule group as a starting point or define a new rule group from scratch. To modify and edit an existing rule group, complete steps 3, 5, 6, and 7. To define a new rule group, complete steps 4, 5, 6, and 7.

3 Create a rule group based on an existing rule group.

a Click **Duplicate** for an existing rule group.

The **Add Rule Group** dialog box appears.

b Specify the rule group name.

c Click **OK**.
The rule group is created and listed on the **Rule Groups** page.

4 Define a new rule group.

a Click **Add Rule Group**.
The **Add Rule Group** dialog box appears.

b Specify the rule group name.

c Select the rule group type and platform.

d Click **OK**.
The rule group is created and listed on the **Rule Groups** page.

5 Click **Edit** for the rule group.

6 Specify the required rules.
For information on the how to define rules, see the *How do I define monitoring rules?* and *How do I define protection rules?* sections.

7 Click **Save Rule Group**.

Importing or exporting rule groups

If you need to replicate the rule group configuration from one McAfee ePO server to another, export the rule group configuration from the (source) McAfee ePO server to an XML file and import the XML file to the (target) McAfee ePO server. You can also export rule groups into an XML file, edit the XML file to make the required changes to rule groups, and import the file to the McAfee ePO server use the changed rule groups.

Use this task to import or export rule groups.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Solidcore Rules**.

2 Complete one of these tasks from the **Rule Groups** tab.

- To import rule groups, click **Import**, browse and select the rule groups file, and click **OK**. While importing, you can specify whether to override rule groups (if you are importing a rule group with the same name as an existing rule group).
- To export selected rule groups to an XML file, select the rule groups, click **Export**, and save the file.

Viewing assignments for a rule group

Instead of navigating through all the created policies, you can directly view all the policies in which a rule group is being used. This feature provides a convenient way to verify if each rule group is assigned to the relevant policies.

Use this task to view the assignments for a rule group.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Solidcore Rules**.

2 Click **Assignments** on the Rule Groups tab to view the policies to which the selected rule group is assigned.

Enabling Change Control

Use this task to enable the Change Control software.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps from the McAfee ePO 4.6 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.

   c Select the **Solidcore 6.0.0** | **SC: Enable** and click **Create New Task**.
   The **Client Task Catalog** page appears.

   d Specify the task name and add any descriptive information.

3 Complete these steps from the McAfee ePO 4.5 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c Specify the task name and add any descriptive information.

   d Select **SC: Enable (Solidcore 6.0.0)** and click **Next**
   The **Configuration** page appears.

4 Select the platform.

5 Select the subplatform (only for the Windows and UNIX platforms).

6 Select the version (only for the Windows platform).

7 Ensure that the **Change Control** option is selected.

8 If you are using Solidcore client version 5.1.5 or earlier, select the **Force Reboot with the task** option to restart the endpoint.
Restarting the system is necessary to enable the software. A popup message is displayed at the endpoint 5 minutes before the endpoint is restarted. This allows the user to save work and data on the endpoint.

9 Click **Save** (McAfee ePO 4.6 only).

10 Click **Next**.
The **Schedule** page appears.

11 Specify scheduling details and click **Next**.

12 Review and verify the task details and click **Save**.

13 Optionally, wake up the agent to send your client task to the endpoint immediately.

Monitoring the file system and registry

Change Control allows you to designate a set of files and registry entries to monitor for changes. You can also choose to track attribute and content changes for monitored files. While you need to define rules to specify the files and registry keys to monitor, user account activity is tracked by default (no rules are needed) for all endpoints on which Change Control is deployed and enabled.

Contents

Understanding monitoring rules

Using rules, you can monitor files, directories, registry keys, file types (based on file extension), programs, and users.

What can I monitor?

The following operations are tracked for a monitored file, registry key, and user account.

Element	Tracked operations
File	• File creation • File modification (file contents and attributes, such as permissions or owner) • File deletion • File rename • Alternate Data Stream creation • Alternate Data Stream modification (contents and attributes, such as permissions or owner) • Alternate Data Stream deletion • Alternate Data Stream rename
Registry key	• Registry key creation • Registry key modification • Registry key deletion
User account	• User account creation • User account modification • User account deletion • User log on (success and failure)

Element	Tracked operations
	• User log off

Are any predefined rules available?

Yes, Change Control includes predefined monitoring rules. For detailed information, see the *Reviewing predefined monitoring rules* section.

Does an order of precedence exist for monitoring rules?

Use the table to understand the order of precedence applied (highest to lowest) when processing monitoring rules.

Table 1: Order of precedence for monitoring rules

Order	Rule Type	Description	
1.	Advanced exclusion filters (AEF) rules have the highest precedence.	For more information on AEF rules, see the *What are advanced exclusion filters or rules (AEFs)?* section.	
2.	Exclude rules are given precedence over include rules.	For example, if you erroneously define an include and exclude rule for the same file, the exclude rule applies.	
3.	Rules based on user name have the precedence over all other rule types except AEF rules.	The user name specified in the rule is compared with the user name referenced in the event.	
4.	Rules based on program name have precedence over rules based on file extension, file name, directory name, or registry key.	The program name specified in the rule is compared with the program name referenced in the event.	
5.	Rules based on file extension have precedence over rules based on file or directory name (or path).	The file extension specified in the rule is compared with file extension referenced in the event. For example, if C:\Program Files\Oracle is excluded from monitoring (by a file-based rule) and the .ora extension is included for monitoring, events will be generated for files with .ora extension, such as listener.ora and tnsnames.ora.	
6.	Rules based on file names or paths have precedence over rules based on directory name. In effect, longer paths take precedence for name-based rules.	The specified path is compared with path referenced in the event. Paths (for files or directories) are compared from the beginning. Consider these examples.	
		Windows platform	If the C:\temp directory is excluded, and the C:\temp\foo.cfg file is included, the changes to the foo.cfg file are tracked. Similarly, if you exclude the HKEY_LOCAL_MACHINE key and include the HKEY_LOCAL_MACHINE\System key, the changes to the HKEY_LOCAL_MACHINE\System key are tracked.
		UNIX platform	If the /usr/dir1/dir2 directory is included and /usr/dir1 directory is excluded, all operations for the files in the /usr/dir1/dir2 directory are monitored because the /usr/dir1/dir2 path is longer and hence, takes precedence.
NOTE: In the afore-mentioned order of precedence, all rules (except #5) apply to registry key rules also.			

What are advanced exclusion filters or rules (AEFs)?

You can define advanced filters to exclude changes by using a combination of conditions. For example, you might want to monitor changes made to the tomcat.log file by all programs except

the tomcat.exe program. To achieve this, define an advanced filter to exclude all changes made to the log file by its owner program. This will ensure you only receive events when the log file is changed by other (non-owner) programs. In this case, the defined filter will be similar to *Exclude all events where filename is <log-file> and program name is <owner-program>*.

Use AEFs to prune routine system-generated change events that are not relevant for your monitoring or auditing needs. Several applications, particularly the web browser, maintain the application state in registry keys and routinely update several registry keys. For example, the ESENT setting is routinely modified by the Windows Explorer application and it generates the Registry Key Modified event. These state changes are routine and need not be monitored and reported upon. Defining AEFs allows you to eliminate any events that are not required for fulfilling compliance requirements and ensures the event list includes only meaningful notifications.

How do I define monitoring rules?

Regardless of whether you create a new monitoring policy or define a monitoring rule group, the framework available to define monitoring rules is the same.

Using variables in rules

The path specified in a monitoring rule can include system environment variables (only on the Windows platform). The following table lists the supported system variables.

Variable	Example value (true for most Windows platforms)
%ALLUSERSPROFILE%	C:\Documents and Settings\All Users
%APPDATA%	C:\Documents and Settings\{username}\Application
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C:
%HOMEPATH%	C:\Documents and Settings\{username}(\ on earlier Windows)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x*86)%	C:\Program Files (x86) (only in 64-bit version)
%SYSTEMDRIVE%	C:
%SYSTEMROOT%	C:\windows (C:\WINNT on earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:\Documents and Settings\{username}\local Settings\Temp C:\Temp
%USERPROFILE%	C:\Documents and Settings\{username} (C:WINNT\profiles\{username} for earlier versions)
%WINDIR%	C:\Windows

Understanding path considerations

These considerations apply to path-based rules.

- Path should be absolute when specifying rules to monitor files and directories.

- Path need not be absolute when specifying rules to monitor program activity. For example, you can specify the partial path, such as AcroRd32.exe or Reader\AcroRd32.exe or fully-qualified path, such as C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe. If you specify the partial path, all programs with names that match the specified string are monitored. If you specify the fully-qualified path, activity is monitored for only the specified program.
- Paths can contain white spaces.
- Paths can include the wildcard character (*). However, it can only represent one complete path component. Here are a few examples.

Windows platform	Using \abc*\def is allowed while \abc*.doc, \abc*.*, or \abc\doc.* is not supported.
UNIX platform	Using /abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* is not supported.

- Paths used in registry key-based rules can include the wildcard character (*). However, the wildcard character can only represent one path component in the registry path. Ensure that you do not use the character for the component at the end of the complete registry path (if used at the end the rule will not be effective).

  Also, at any time, the CurrentControlSet in the Windows Registry is linked to the relevant HKEY_LOCAL_MACHINE\SYSTEM\ControlSetXXX key. For example, the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet can be linked to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001 key. When a change is made to either link, it is automatically updated on both the links. For a monitored key, events are always reported with the path of CurrentControlSet and not ControlSetXXX.

Defining monitoring rules

Use this table to define monitoring rules. You can perform these actions when creating or modifying a monitoring (Integrity Monitor) policy or rule group.

Table 2: Defining Monitoring Rules

Action	Steps
Monitor files and directories	1. Click **Add** on the **File** tab. The **Add File** dialog box appears. 2. Specify the file or directory name. 3. Indicate whether to include for or exclude from monitoring. 4. Optionally, to track content and attribute changes for a file, select **Enable File Tracking** and specify the file encoding. 5. Click **OK**.
Monitor registry keys (Windows platform only)	1. Click **Add** on the **Registry** tab. The **Add Registry** dialog box appears. 2. Specify the registry key. 3. Indicate whether to include for or exclude from monitoring and click **OK**.
Monitor specific file types	1. Click **Add** on the **Extension** tab. The **Add Extension** dialog box appears. 2. Type the file extension. Do not include the period (dot) in the extension. For example, log. 3. Indicate whether to include for or exclude from monitoring and click **OK**.
Monitor program activity (in effect choose to track or not track all file or registry changes made by a program)	1. Click **Add** on the **Program** tab. The **Add Program** dialog box appears. 2. Enter the name or full path of the program. 3. Indicate whether to include for or exclude from monitoring and click **OK**. We recommend that you exclude background processes, such as the lsass.exe process.

Action	Steps
Specify the users to **exclude** from monitoring (in effect all changes made by the specified user are not tracked)	1. Click **Add** on the **User** tab. The **Add User** dialog box appears. 2. Specify the user name. Consider the following: • Spaces in user names should be specified within quotes. • Domain name can be a part of the user name on the Windows platform. If the domain name is not specified, the user name is excluded from monitoring for all domains. • Exclude all users in a particular domain (on the Windows platform) by using MY-DOMAIN* or *@MY-DOMAIN. 3. Click **OK**.
Specify advanced exclusion filters	1. Click **Add Rule** on the **Advanced** tab. A new filter row appears. You can create filters based on files, events, programs, registry keys, and users. 2. Edit the settings to specify the filter. 3. Click **+** or **Add Rule** to specify additional AND or OR conditions, respectively. You can also define AEFs from the **Events** page. For more information, see the *Excluding events* section.

Reviewing predefined monitoring rules

Change Control provides multiple predefined filters suitable for monitoring relevant files on various operating systems. By default, these filters are applied to the global root in the system tree and hence are inherited by all McAfee ePO-managed endpoints on which Change Control is installed. As soon as an endpoint connects to the McAfee ePO server, the Minimal System Monitoring policy applicable to the endpoint's operating system comes into play.

Use this task to review the predefined filters included in the Minimal System Monitoring policy (applicable to your operating system).

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. Select the **Solidcore 6.0.0: Integrity Monitor** product.
   All policies for all categories are listed. Note that a **Minimal System Monitoring** policy exists for each supported operating system.
3. Open the relevant **Minimal System Monitoring** policy.
   By default, the *My Rules* rule group is open (which is blank).
4. Select a rule group in the **Rule Groups** pane to review the filters included in the rule group.

   NOTE: To override any rules included in the **Minimal System Monitoring** policy, you can duplicate the relevant rule group (in which the required rules are present), edit the rule group to add the new rules, and add the rule group to a policy. For most other purposes, ensure that the **Minimum System Monitoring** policy is applied on the endpoints and additional rules are applied by using a separate policy.
5. Click **Cancel**.

Creating monitoring policies

Using a monitoring policy, you can choose to monitor changes or exclude from monitoring various units of a file system and registry. You can control monitoring of files, directories, registry keys, file types (based on file extension), programs, and users. These are multi-slot policies; a user can assign multiple policies to a single node in the system tree.

To create a monitoring policy, you can either define rules in a rule group (to allow reuse of rules) and add the rule group to a policy or define the rules directly in a policy. Use this task to create a new monitoring policy.

Before you begin

Review these guidelines before you define monitoring rules.

1. Identify key applications installed on the endpoint.
2. Create a policy to monitor each key application (file, registry key, extension, program, user, and advanced rules). A typical way to do this could be to:
   - Include the install directory, registry keys, and configuration files.
   - Exclude the log files (by defining AEF rules). For more information on AEF rules, see the *What are advanced exclusion filters or rules (AEFs)?* section.
   - Exclude the process of the application.
3. Assign the policy to one or more endpoints and check periodically for events.
4. Test and refine the policy, as needed. Exclude any events that are generated regularly during the routine operation of an application and are unimportant.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. Select the **Solidcore 6.0.0: Integrity Monitor** product.
3. Click **Actions** | **New Policy**.
   The **New Policy** dialog box appears.
4. Select the category.
5. Select the policy you want to duplicate from **Create a policy based on this existing policy** list.
6. Specify the policy name and click **OK**.
   The **Policy Settings** page opens. You can now define the rules to include in the policy. You can either add existing rule groups to the policy or directly add the new rules to the policy.
   - To use a rule group, complete steps 7 and 9. For more information on how to create a rule group, see the *Creating rule groups* section.
   - To directly add the rules to the policy, complete steps 8 and 9.
7. Add a rule group to the policy.
   a. Select the rule group in the **Rule Groups** pane.
   The rules included in the rule group are displayed in the various tabs.
   b. Review the rules.
   c. Click **Add** in the **Rule Groups** pane.
   The **Select Rule Groups** dialog box appears.

d Select the rule group to add.

e Click **OK**.

8 Add the monitoring rules to the policy.
For information on the how to define rules, see the *How do I define monitoring rules?* section.

9 Save the policy.

Managing content changes

Using Change Control, you can track content and attribute changes for a monitored file. If you enable content change tracking for a file, any attribute or content change to the file creates a new file version at McAfee ePO. You can view and compare the different versions that are created for a file. You can also compare any two files or file versions that exist on the same or different endpoints. You can also configure an Automatic Response to send an email whenever a critical file is modified (the email will highlight the exact changes made to the file).

Contents

Tracking content changes

Use this task to track content changes for files. You can perform these actions when creating or modifying a monitoring (Integrity Monitor) policy or rule group.

Task

For option definitions, click **?** in the interface.

1 Navigate to the **File** tab.

2 Perform one of these steps.

- Click **Add** to monitor and track changes for a new file.
- Select an existing rule and click **Edit**.

The **Add File** dialog box appears.

3 Review or add the file information.

4 Select the **Enable Content Change Tracking** option.

5 Select the file encoding.
You can choose between Auto Detect, ASCII, UTF-8, and UTF-16. Auto Detect works for most files. If you are aware of the file encoding, select ASCII, UTF-8, or UTF-16 (as appropriate). If needed, you can add new file encoding values. Contact McAfee Support for assistance in adding a file encoding value.

6 Click **OK**.

NOTE: You cannot track changes for directories or network files.

Managing file versions

Use this task to review all versions available for a file, compare file versions, reset the base version, and delete versions. The base version identifies the starting point or initial document to use for comparison or control. Typically, the oldest version of a file is set as the base version. In effect, when you start tracking changes for a file, the initial file content and attributes are stored on the McAfee ePO database and set as the base version.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting** | **Content Change Tracking**.
   All files for which content change tracking is enabled are listed.
2. Identify the file for which to review versions.
   - Specify the endpoint or file name in the Quick find text box and click **Apply**. The list is updated based on the specified search string.
   - Sort the list based on the system name, file name, or status.
3. Review the file status.
   The File Status column denotes the current status of content change tracking. Possible status values include:

Success	Indicates that content changes for the file are being tracked successfully.
File not found	Indicates that the file was not found at the specified path. Verify the file exists and check the specified path.
Content change tracking is not supported for a directory	Indicates that the file specified for content tracking is a directory. Note that you cannot track changes for directories.
Content change tracking is not supported for file name with wildcard	Indicates that the specified file path includes wildcard characters. Note that you cannot use wildcard characters while specifying the file path for content change tracking.
File size exceeds maximum size limit	Indicates that the file size has exceeded the specified size limit for content change tracking. If needed, you can change the size limit for content change tracking for the endpoints. For more information, see the *Specifying maximum file size* section.
File removed from content change tracking	Indicates that the file has been removed from content change tracking and further changes to the file will not generate a new version.
Content change tracking is not supported for files on a network volume	Indicates that the file specified for content tracking is stored on a network volume. Note that you cannot track changes for files on network volumes.
Content change tracking is not supported for encrypted file	Indicates that the file specified for content tracking has been encrypted on the endpoint.
File Deleted	Indicates that the file specified for content tracking has been deleted from the endpoint.
File Renamed	Indicates that the file specified for content tracking has been renamed on the endpoint.
Multiple file encodings defined	Indicates that multiple and conflicting file encoding values are specified for the file. This can occur if two monitoring rules, each with a different file encoding value, are applied to track content changes for the file.

4. Click **View revisions**.
   The File revisions page displays all versions for the file. From this page you can compare file versions, specify the base version, and delete file versions from the McAfee ePO database.
5. Compare the file versions.

a Specify what to compare.

- Click **Compare with previous** for a version to compare that version with the previous version of the file available at the ePO console.
- Click **Compare with base** for a version to compare that version with the base version.
- Select any two versions (by clicking the associated check boxes) and select **Actions** | **Compare Files** to compare the selected versions.

The versions are compared and differences between the file content and file attributes are displayed.

b Click **Close**.

6 Reset the base version.

a Select a file version to set as the base version (by clicking the associated check box).

b Select **Actions** | **Set as base version**.

c Click **OK**.
This resets the base version and deletes all previous versions (older than the new base version) of the file.

NOTE: At a time, the software can track up to 200 versions for a file. If the number of versions exceeds 200, the application deletes the oldest versions to bring the version count to 200. Then, it automatically sets the oldest version as the base version. If needed, you can configure the number of versions to maintain for a file. Contact McAfee Support for assistance in configuring the number of versions to maintain for a file.

7 Delete file versions.
Deleting file versions removes the selected file versions from the McAfee ePO database. It does not alter or remove the actual file present on the endpoint.

a Select one or more file versions by clicking the associated check boxes.

b Select **Actions** | **Delete**.

c Click **OK**.

8 Click **Close**.

Comparing files

Use this task to compare any two files (or file versions) on an endpoint or on two different endpoints.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Reporting** | **Content Change Tracking**.

2 Click **Advanced File Comparison**.

3 Specify information for file 1.

a Select the group from the list.

b Enter the host name.

c Enter the name and path of the file.

d Select the version to compare.

4 Specify information for file 2.

5 Click **Show Comparison**.
The files (attributes and content) are compared and differences are displayed.

6 Review the results.

7 Click **Close**.

Receiving change details by email

To closely observe changes to a critical file, you can choose to receive an email (with change details) each time the file is changed.

Use this task to receive an email each time a change is made to a file for which you are tracking content changes.

Before you begin

Ensure that the email server is configured.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Automation** | **Automatic Responses**.

2 Click **Actions** | **New Response**.
The **Response Builder** page opens to the **Description** page.

3 Enter the response name.

4 Select the **Solidcore Events** group and **File Content Change Event** type.

5 Select **Enabled**.

6 Click **Next**.
The **Filter** page appears.

7 Specify the file name, system name, or both.

- To receive an email each time a specific tracked file changes (across all managed endpoints), specify only the file name.
- To receive an email each time any tracked file changes on an endpoint, specify only the system name.
- To receive an email each time a specific file on an endpoint is changed, specify both file and system name.

8 Click **Next**.
The **Aggregation** page appears.

9 Specify aggregation details and click **Next**.
The **Actions** page appears.

10 Select Send File Content Change Email, specify the email details, and click **Next**.
The **Summary** page appears.

11 Review the details and click **Save**.

Specifying maximum file size

By default, you can track changes for any file with a size of 1000 KB or lower. If needed, you can configure the maximum file size for tracking content changes.

NOTE: Modifying the maximum file size will affect the McAfee ePO database sizing requirements.

Use this task to specify the maximum file size to track content changes.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. Select the **Solidcore 6.0.0: General** product.
   The **McAfee Default** policy includes customizable configuration settings.
3. Click **Duplicate** for the McAfee Default policy in the Configuration (Client) category.
   The **Duplicate Existing Policy** dialog box appears.
4. Specify the policy name and click **OK**.
   The policy is created and listed on the **Policy Catalog** page.
5. Open the policy.
   - If you are using McAfee ePO 4.6, click the new policy.
   - If you are using McAfee ePO 4.5, click **Edit Settings** for the policy.
6. Switch to the **Miscellaneous Settings** tab.
7. Specify the file size.
8. Save the policy and apply to the relevant endpoints.

Protecting the file system and registry

Using Change Control, you can prevent changes to the file system and registry.

Contents

Understanding protection rules

To prevent unauthorized access and changes, you define read-protection and write-protection rules.

Read-protection rules	Prevent users from reading the content of specified files, directories, and volumes. When a directory is read protected, all files in the directory are read protected. Any unauthorized attempt to read data from protected files is prevented and an event is generated. Writing to read-protected files is allowed. NOTE: You cannot define read-protection rules for registry keys.
Write-protection rules	Prevent users from creating new files (including directories and registry keys) and modifying existing files, directories, and registry keys. • Define write-protection rules for files and directories to protect them from unauthorized modifications. Only protect critical files. When a directory is included for write protection, all files contained in that directory and its subdirectories are write protected. • Define write-protection rules for critical registry keys to protect them against change.

Can I override defined rules?

While you can define rules to protect, you can also define additional rules to selectively override the read or write protection that is in effect.

- Specify programs that are permitted to selectively override the read or write protection.
- Specify users (on the Windows platform only) who are permitted to selectively override the read or write protection.

Does an order of precedence exist for protection rules?

These considerations are used when protection rules are applied at the endpoint:

- Exclude rules are given precedence over include rules.

  For example, if you erroneously define an include and exclude rule for the same file, the exclude rule applies.

- Longer paths are given precedence.

  For example, if C:\temp is included for write protection, and C:\temp\foo.cfg is excluded, the changes to foo.cfg are permitted. Similarly, if you exclude HKEY_LOCAL_MACHINE and include HKEY_LOCAL_MACHINE\System for write protection, the changes to HKEY_LOCAL_MACHINE\System are prevented.

How do I define protection rules?

Regardless of whether you use a rule group or policy, the framework available to define protection rules is the same.

Using variables in rules

The path specified in a protection rule can include system environment variables (only on the Windows platform). The following table lists the supported system variables.

Variable	Example value (true for most Windows platforms)
%ALLUSERSPROFILE%	C:\Documents and Settings\All Users
%APPDATA%	C:\Documents and Settings\{username}\Application
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C:
%HOMEPATH%	C:\Documents and Settings\{username}(\ on earlier Windows)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x*86)%	C:\Program Files (x86) (only in 64-bit version)
%SYSTEMDRIVE%	C:
%SYSTEMROOT%	C:\windows (C:\WINNT on earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:\Documents and Settings\{username}\local Settings\Temp C:\Temp
%USERPROFILE%	C:\Documents and Settings\{username} (C:WINNT\profiles\{username} for earlier versions)
%WINDIR%	C:\Windows

Understanding path considerations

These considerations apply to path-based rules.

- Path should be absolute when specifying rules to read or write-protect files and directories.
- Path need not be absolute when specifying rules to add a trusted program or updater. For example, you can specify the partial path, such as AcroRd32.exe or Reader\AcroRd32.exe or fully-qualified path, such as C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe. If you specify the partial path, all programs with names that match the specified string are added as trusted programs. If you specify the fully-qualified path, only the specified program is added as a trusted program.
- Paths can contain white spaces.

- Paths can include the wildcard character (*). However, it can only represent one complete path component. Here are a few examples.

Windows platform	Using \abc*\def is allowed while \abc*.doc, \abc*.*, or \abc\doc.* is not supported.
UNIX platform	Using /abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* is not supported.

- Paths used in registry key-based rules can include the wildcard character (*). However, the wildcard character can only represent one path component in the registry path. Ensure that you do not use the character for the component at the end of the complete registry path (if used at the end, the rule will not be effective).

Defining protection rules

Use this table to define protection rules. You can perform these actions when modifying or creating a protection (Change Control) policy or rule group.

Table 3: Defining Protection Rules

Action	Steps
Read-protect files and directories	1. Click **Add** on the **Read Protect** tab. The **Add File** dialog box appears. 2. Specify the file or directory name. 3. Indicate whether to include for or exclude from read protection. 4. Click **OK**. NOTE: By default, the read protection feature is disabled at the endpoints.
Write-protect files and directories	1. Click **Add** on the **Write Protect File** tab. The **Add File** dialog box appears. 2. Specify the file or directory name. 3. Indicate whether to include for or exclude from write protection. 4. Click **OK**.
Write-protect registry keys	1. Click **Add** on the **Write Protect Registry** tab. The **Add Registry** dialog box appears. 2. Specify the registry key. 3. Indicate whether to include for or exclude from write protection. 4. Click **OK**.
Specify trusted programs permitted to override the read and write protection rules	1. Click **Add** on the **Updaters** tab. The **Add Updater** dialog box appears. 2. Specify the location of the binary file. 3. Enter a unique identification label for the executable file. For example, if you specify **Adobe Updater Changes** as the identification label for the Adobe_Updater.exe file, all change events made by the Adobe_Updater.exe file will be tagged with this label. 4. Specify conditions that the binary file must meet to run as an updater. • Select **None** to allow the binary file to run as an updater without any conditions. • Select **Parent** to allow the binary file to run as an updater only if it is launched by the specified parent. For example, when configuring updater.exe as an updater to allow changes to Mozilla Firefox, specify firefox.exe as the parent. Although updater.exe is a generic name that can be part of any installed application, using the parent ensures that only the correct program is allowed to run as an updater. • Select **Library** to allow the binary file to run as updater only when it has loaded the specified library. For example, when configuring iexplore.exe as an updater to allow Windows Updates using Internet Explorer, specify wuweb.dll as the library. This ensures that the iexplore.exe program has updater privileges only till the web control library (wuweb.dll) is loaded. 5. Indicate whether to disable inheritance for the updater. For example, if Process A (that is set as an updater) launches Process B, disabling inheritance for Process A ensures that Process B will not become an updater.

Action	Steps
	6. Indicate whether to suppress events generated for the actions performed by the updater. Typically, when a updater changes a protected file, a File Modified event is generated for the file. If you select this option, no events are generated for changes made by the updater.
Specify authorized users permitted to override the read and write protection rules	You can either enter user details or import user or group details from an Active Directory. Ensure that the Active Directory is configured as a registered server. Specify details to authorize users to override the read or write protection rules. (Windows only) 1. Click **Add** on the **Trusted User** tab. The **Add User** dialog box appears. 2. Enter the domain and logon name of the user. 3. Specify a unique identification label for the user. For example, if you specify **John Doe Changes** as the identification label for the John Doe user, all changes made by the user will be tagged with this label. 4. Type the user name. 5. Click **OK**.
	Import user details from an Active Directory. 1. Click **AD Import** on the **Trusted User** tab. The **Import from Active Directory** dialog box appears. 2. Select the server. 3. Select **Global Catalog Search** to search for users in the catalog (only if the selected Active Directory is a Global Catalog server). 4. Specify whether to search for users based on the UPN (User Principal Name) or SAM account name. Note that your search will determine the authorized user. Ensure that you use the trusted account to log on to the endpoint. If you use the UPN name while adding a user, ensure that the user logs on with the UPN name at the endpoint to enjoy trusted user privileges. 5. Enter the user name. The **Contains** search criteria is applied for the specified user name. 6. Specify a group name to search for users within a group. NOTE: You cannot directly add a group present in the Active Directory to a policy. To authorize all users in a group, add the user group to a rule group and include the rule group in a policy. Using groups ensures that all changes to a user group automatically cascade across all rule groups and associated policies. 7. Click **Find**. The search results are displayed. 8. Select the users to add in the search results and click **OK**.

Creating a protection policy

Use this task to create a new protection policy. These are multi-slot policies; a user can assign multiple policies to a single node in the system tree.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. Select the **Solidcore 6.0.0: Change Control** product.
3. Click **New Policy**.
   The **New Policy** dialog box appears.

4 Select the category.

5 Select the policy you want to duplicate from **Create a policy based on this existing policy** list.

6 Specify the policy name and click **OK**.
The **Policy Settings** page opens.

7 Specify protection rules.

NOTE: The read-protect feature is disabled by default. To use read-protection rules, enable the read-protect feature for the endpoints.

8 Save the policy.

Enabling read protection

By default, the read-protect feature is disabled for optimal system performance. Use this task to run a command on the endpoint to enable read protection.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps from the McAfee ePO 4.6 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Client Task Assignment**.
The **Client Task Assignment Builder** page appears.

c Select the **Solidcore 6.0.0** product, **SC: Run Commands** task type, and click **Create New Task**.
The **Client Task Catalog** page appears.

d Specify the task name and add any descriptive information.

3 Complete these steps from the McAfee ePO 4.5 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Task**.
The **Client Task Builder** page appears.

c Specify the task name and add any descriptive information.

d Select **SC: Run Commands (Solidcore 6.0.0)** and click **Next**
The **Configuration** page appears.

4 Type the following command.
features enable deny-read

5 Select **Requires Response** if you want to view the status of the commands in **Menu** | **Change Control** | **Client Task Log** tab.

6 Click **Save** (McAfee ePO 4.6 only).

7 Click **Next**.
The **Schedule** page appears.

8 Specify scheduling details and click **Next**.

9 Review and verify the task details and click **Save**.

10 Optionally, wake up the agent to send your client task to the endpoint immediately.

Monitoring and reporting

When a monitored file or registry key is changed or an attempt is made to access or change a protected resource, an event is generated on the endpoint and sent to the McAfee ePO server. Review and manage the generated events to monitor the network status. You can also use customizable dashboards to monitor critical security status "at-a-glance," and report that status to stakeholders and decision makers using preconfigured queries.

Contents

Managing events

View and manage the events from the McAfee ePO console.

Contents

Reviewing events

Use this task to review the events.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting** | **Solidcore Events**.
2. Specify the time duration for which to view events by selecting an option from the **Time Filter** list.
3. Specify the endpoints for which to view events.
   a. Select the required group in the **System Tree**.
   b. Select an option from the **System Tree Filter** list.
4. Optionally, view only specific events by applying one or more filters.
   a. Click **Advanced Filters**.
   The **Edit Filter Criteria** page appears.
   b. Select an available property.

c Specify the comparison and value for the property.
For example, to view only File Modified events, select the Event Display Name property, set comparison to Equals, and select the File Modified value.

d Click **Update Filter**.
Events matching the specified criteria are displayed.

5 View details for an event by clicking the corresponding row.

6 Review endpoint details for one or more events.

a Select one or more events.

b Click **Actions** | **Show Related Systems**.
The **Related Systems** page lists the endpoints corresponding to the selected events.

c Click a row to review detailed information for the endpoint.

d Optionally, perform any action on the endpoint.

Viewing content changes

An event is generated each time the attributes or contents change for a file that is being tracked for changes. Based on the change made to the file, one of these events is generated:

- FILE_CREATED
- FILE_DELETED
- FILE_MODIFIED
- FILE_RENAMED
- FILE_ATTR_MODIFIED
- FILE_ATTR_SET
- FILE_ATTR_CLEAR
- ACL_MODIFIED
- OWNER_MODIFIED

If any of the afore-mentioned events is generated for a file for which you are tracking content changes, you can review details of the change made to the file. Use this task to view details of changes made to a file for which you are tracking content changes.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Reporting** | **Solidcore Events**.

2 Click **View Content Change** for the event.
The page compares two versions of the file.

3 Review the host, file attribute, and file content information.
Not that the change made to the file is highlighted.

4 Click **Close**.

Excluding events

You can define rules to prune routine system-generated change events not relevant for monitoring or auditing.

Use this task to exclude or ignore events not required to meet compliance requirements.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting** | **Solidcore Events**.
2. Select the events to exclude.
3. Click **Actions** | **Exclude Events**.
   The **Events Exclusion Wizard** appears.
4. Select the target platform for the rules.
5. Select the rule group type and click **Next**.
   The **Define Rules** page appears.
6. Rules are auto-populated based on the selected events.
7. Review and refine existing rules and add new rules, as needed.
8. Click **Next**.
   The **Select Rule Group** page appears.
9. Add the rules to an existing or new rule group and click **Save**.
10. Ensure the rule group is added to the relevant policy and the policy is assigned to the endpoints.
    Once excluded, similar new events are no longer displayed on the McAfee ePO console. Excluding events does not remove the existing or similar events on the **Events** page.

Using dashboards

Dashboards are collections of monitors that help you keep an eye on your environment. Change Control provides these default dashboards:

- **Solidcore: Integrity Monitor** dashboard allows you to observe the monitored endpoints
- **Solidcore: Change Control** dashboard helps you keep a check on the protected endpoints

You can create, modify, duplicate, and export dashboards. For more information on working with dashboards, see the *McAfee ePolicy Orchestrator Software Product Guide*.

Viewing queries

Use the available queries to review information for the endpoints based on the data stored in the McAfee ePO database. The following Change Control queries are available from the McAfee ePO console.

Table 4: Change Control Queries

Query	Description
Solidcore: Alerts	Displays all alerts generated in the last 3 months.
Solidcore: Attempted Violations Detected in the Last 24 Hours	Displays the attempted violation events detected during the last 24 hours. The line chart plots data on a per hour basis. Click a value on the chart to review event details.
Solidcore: Attempted Violations Detected in the Last 7 Days	Displays the attempted violation events detected during the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review event details.

Query	Description
Solidcore: Integrity Monitor Status Report	Displays the status of all endpoints with the Change Control license which are managed by the McAfee ePO console. The pie chart categorizes the information based on the client status. Click a segment to review endpoint information.
Solidcore: Agent Status Report	Displays the status of all endpoints managed by the McAfee ePO console. This report combines information for both the Application Control and Change Control licenses. The pie chart categorizes the information based on the client status. Click a segment to review detailed information.
Solidcore: Agent License Report	Indicates the number of Solidcore Agents that are managed by the McAfee ePO console. The information is categorized based on the license information, namely Application Control and Change Control, and further sorted based on the operating system on the endpoint.
Solidcore: Integrity Monitor Events Detected in the Last 24 Hours	Displays monitoring-related events detected during the last 24 hours. The line chart plots data on a per hour basis. Click a value on the chart to review event details.
Solidcore: Integrity Monitor Events Detected in the Last 7 Days	Displays monitoring-related events detected during the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review event details.
Solidcore: Non Compliant Solidcore Agents	Lists the endpoints that are currently not compliant. The list is sorted based on the reason for non-compliance. An endpoint can be non compliant if it is in Disabled or Update mode or if the local Command Line Interface (CLI) access is recovered.
Solidcore: Out of Band Change Events detected in Last 24 Hours	Displays change events generated in the last 24 hours which are not compliant with the update policy. The line chart plots data on a per hour basis. Click a value on the chart to review event details.
Solidcore: Out of Band Change Events detected in Last 7 Days	Displays change events generated in the last 7 days which are not compliant with the update policy. The line chart plots data on a per day basis. Click a value on the chart to review event details.
Solidcore : PCI Req 10.3: File Integrity Monitoring - Rolling 90 Days	Displays the summary of changes that are grouped by the program name. This report allows you to comply with Payment Card Industry (PCI) requirement 10.3.
Solidcore : PCI DSS Req 11.5: Detailed PCI File Integrity Monitoring - Rolling 90 Days	Displays a detailed audit log of the critical systems, critical applications, and configuration files. This report allows you to comply with PCI Data Security Standards (DSS) requirement 11.5.
Solidcore : PCI DSS Req 11.5: Summary PCI File Integrity Monitoring - Rolling 90 Days	Displays a summarized audit log of the critical systems, critical applications, and configuration files. This report allows you to comply with PCI DSS requirement 11.5.
Solidcore : PCI DSS Req 10.3.1: User Report Detail - Rolling 90 Days	Displays a detailed list of changes that are grouped by the user name. This report allows you to comply with PCI DSS requirement 10.3.1.
Solidcore : PCI DSS Req 10.3.1: User Report Summary - Rolling 90 Days	Displays the summarized list of changes that are sorted based on the user name and date. This report allows you to comply with PCI DSS requirement 10.3.1.
Solidcore: Policy Assignments By System	Lists the number of policies applied on the managed endpoints. Click a system to review information on the applied policies.
Solidcore: Policy Details	Categorizes and lists the rules defined in a selected monitoring or protection policy. To view the report, click **Edit** for the query, navigate to the Filter page, select a policy name, and click **Run**. Click a category to review all the rules in the category.
Solidcore: Top 10 Change Events in the Last 7 Days	Displays the top 10 change events that were generated during the last 7 days. The chart includes a bar for each event type and indicates the number of events generated for each event type. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.

Query	Description
Solidcore: Top 10 Programs with Most Change Events in the Last 7 Days	Displays the top 10 programs with most changes during the last 7 days. The chart includes a bar for each program and indicates the number of events generated by each program. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Systems with Most Change Events in the Last 7 Days	Displays the top 10 systems with the most changes during the last 7 days. The chart includes a bar for each system and indicates the number of events generated for each system. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Systems with Most Violations Detected in the Last 24 Hours	Displays the top 10 systems with the maximum number of violations in the last 24 hours. The chart includes a bar for each system and indicates the number of violations for each system. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Systems with Most Violations Detected in the Last 7 Days	Displays the top 10 systems with the maximum number of violations in the last 7 days. The chart includes a bar for each system and indicates the number of violations for each system. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Users with Most Change Events in the Last 7 Days	Displays the top 10 users with the most changes during the last 7 days. The chart includes a bar for each user and indicates the number of events generated by each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Users with Most Violations Detected in the Last 24 Hours	Displays the top 10 users with the most policy violation attempts in the last 24 hours. The chart includes a bar for each user and indicates the number of policy violation attempts for each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Users with Most Violations Detected in the Last 7 Days	Displays the top 10 users with the most policy violation attempts in the last 7 days. The chart includes a bar for each user and indicates the number of policy violation attempts for each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.

Use this task to view a query.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting.**
2. Perform one of these tasks.
   - From the McAfee ePO 4.6 console, select **Queries & Reports**.
   - From the McAfee ePO 4.5 console, select **Queries**.
3. Select the **Change Control** group under **Shared Groups**.
4. Review the queries in the list.
5. Navigate to the required query and click **Run**.
   The results for the selected query are displayed.
6. Click **Close** to return to the previous page.

Getting started with Application Control

Before you begin using Application Control, get familiar with it and understand related concepts.

Contents

Understanding Application Control modes

At any time, Application Control can operate in one of these modes.

Enabled

Indicates that the application is in effect and no unauthorized changes are allowed on the endpoints. When in Enabled mode, Application Control:

- Allows only authorized applications to run on servers and endpoints
- Prevents all unauthorized code including binaries and scripts from running
- Protects against memory-based attacks and application tampering

Enabled mode is the recommended mode of operation. From the Enabled mode, you can switch to the Disabled, Update, or Observe mode.

Observe

Indicates that the application is in effect but is not preventing any changes made on the endpoints. Using the Observe mode is similar to doing a *dry run* for Application Control. Observe mode is available only on the Windows platform.

When running in Observe mode, Application Control emulates the Enabled mode but logs observations instead of preventing any applications or code from running. An observation is logged corresponding to each action Application Control will take when in Enabled mode. For example, if not authorized, the execution of the Adobe Reader application will be prevented in Enabled mode. In Observe mode, the Adobe Reader application is allowed to execute and an observation is generated to indicate that the execution was permitted.

You can place Application Control in Observe mode to:

- Check the compatibility of Application Control with existing software during initial deployment
- Test an application prior to enterprise-wide deployment on endpoints already running Application Control

If you switch to the Observe mode from the Disabled mode, the endpoints need to be restarted. From the Observe mode, you can switch to the Enabled or Disabled mode. When switching to Enabled or Disabled mode, you can choose to either allow or discard all changes made during Observe mode (all changes made in Observe mode are tracked). For more information on the Observe mode, see the *Deploying Application Control in Observe mode* section.

Update

Indicates that the application is in effect, allows ad-hoc changes to the system, and tracks the changes made to the endpoints. We recommend that you use the Update mode only for installing minor software updates. Only use the Update mode to perform scheduled or emergency changes that cannot be made

when Application Control is running in Enabled mode. Note that whenever possible utilize other preferred methods, such as trusted users, directories, publishers or installers to allow changes.

In the Enabled mode, if you install any new software or add new binary files, the files will not be added to the whitelist or allowed to execute (unless performed by trusted change method). However, if you install or uninstall software or add new binary files in the Update mode, all changes are tracked and added to the whitelist.

To authorize or approve changes to endpoints, a change window is defined during which users and programs can make changes to the endpoint. In effect, the Update mode allows you to schedule software and patch installations, remove or modify software, and dynamically update the local whitelist. The application generates the FILE_SOLIDIFIED event for files added during Update mode and FILE_UNSOLIDIFIED event for files deleted during Update mode. Also, when an endpoint is in Update mode, all changes to existing files in the inventory generate corresponding update mode events, such as FILE_MODIFIED_UPDATE and FILE_RENAMED_UPDATE.

NOTE: Memory-protection techniques are enabled in Update mode. This ensures that running programs cannot be exploited.

From the Update mode, you can switch to the Enabled or Disabled mode.

Disabled	Indicates that the application is not in effect. Although the application is installed, the associated features are not active. When you switch to the Disabled mode, the endpoints need to be restarted. From the Disabled mode, you can switch to the Enabled, Update, or Observe mode.

Managing protected endpoints

When you deploy Application Control to protect an endpoint, it creates a whitelist of all executable binary and script files present on the endpoint. The whitelist lists all authorized files and is used to determine trusted or known files. In Enabled mode, only files present in whitelist are allowed to execute. Also, all files in the whitelist are protected and cannot be modified or deleted. An executable binary or script file that is not in the whitelist is said to be unauthorized and is prevented from running.

Authorizing files and programs

The whitelist is the most-common method to determine trusted or known files. You can authorize a program or file on a protected endpoint by using one of these methods:

1. By checksum
2. By certificate or publisher
3. By name
4. By adding to the whitelist

The order in which the methods are listed indicates the precedence the software applies to the methods. For example, if you ban a program based on its checksum value and it is present in the whitelist (and hence is authorized), the program is banned. Similarly, if a program is allowed based on its checksum value and is banned by name, the program will be allowed to execute and run.

Allowing changes to endpoints

Typically, most applications and executable files remain unchanged over prolonged periods of time. However, if needed, you can allow certain applications and executable files to create, modify, or delete files in the whitelist. To design a trust model and allow additional users or programs to modify a protected endpoint, you can use one these methods.

Updater	Refers to an application permitted to update the endpoint. If a program is configured as an updater, it is allowed to install new software and update existing software. For example, if you configure Adobe 8.0 updater program as an updater, it can periodically patch all needed files. NOTE: Updaters work at a global-level and are not application- or license-specific. After a program is defined as an updater, it can modify any protected file. If you are using both Application Control and Change Control, an updater defined via an Application Control policy will also be able to modify files protected by rules defined in a Change Control policy. Note that an updater is not authorized automatically. To be authorized, an updater must be present in the whitelist or given explicit authorization (defined as an allowed binary via a policy). We recommend that you use caution and judiciously assign updater privileges to binary files. For example, if you set cmd.exe as an updater and invoke any executable from it, the executable can perform any change on the protected endpoints. NOTE: To avoid a security gap it is **not** recommended to have a file configured as an allowed binary and updater concurrently. Common candidates to set as updaters include software distribution applications, such as Tivoli, Opsware, Microsoft Systems Management Server (SMS), and Bladelogic and programs that need to frequently update themselves. Application Control includes predefined rules for commonly-used applications that might need to update the endpoints frequently. For example, rule groups are defined for the Altiris, SCCM, and McAfee products.
Publisher	Refers to a publisher or trusted certificate (associated with a software package) that is permitted to run on a protected endpoint. After you add a certificate as a publisher, you can run all software that is signed by the certificate. For example, if you add Adobe's code signing certificate as a publisher, all software issued by Adobe and signed by Adobe's certificate will be permitted to run. To allow any custom scripts and in-house applications to run on protected endpoints, you can sign the scripts and applications with an internal certificate and define the internal certificate as a trusted publisher. After you do so, all applications signed by the certificate are allowed. Also, all applications and binary files either added or modified on an endpoint that are signed by the certificate are automatically added to the whitelist. When adding a publisher, you can also choose to provide updater privileges to the publisher. We recommend that you use this option judiciously because selecting this option will ensure that all the binary files signed by publisher acquire updater privileges. For example, if you set the Microsoft certificate that signs the Internet Explorer application as an updater, Internet Explorer can download and execute any application from the internet. In effect, any files added or modified by an application that is signed by the publisher (with updater privileges) will be added to the whitelist automatically.
Installer	Refers to an application installer identified by its checksum (SHA1) that is allowed to install or update software. When a program (or an installer) is configured as an authorized installer, it gets both the attributes - authorized binary and updater. Hence, regardless of whether the installer was originally present on the endpoint or not, it is allowed to execute and update software on the endpoint. An authorized installer is allowed on the basis of the checksum (SHA1) value of the installer (specified while configuring the policy). This ensures that regardless of the source of installer (and how one gets this installer to the endpoint), if the checksum value matches, the installer will be allowed to run. For example, if you add the installer for the Microsoft Office 2010 suite as an installer, if the checksum matches the installer will be allowed to install the Microsoft Office suite on the protected endpoints.
Trusted Directory	Refers to a directory (local or network share) identified by its Universal Naming Convention (UNC) path. After you add a directory as a trusted directory, endpoints are permitted to run any software present on that directory. When enabled, Application Control prevents protected endpoints from executing any code residing on a network share. If you maintain shared folders containing installers for licensed applications on the internal network in your organization, add trusted directories for such network shares. Additionally, if needed, you can also allow the software located at that UNC path to install software on the protected endpoints. For example, when logging on to a Domain Controller from a protected endpoint, you will need to define \\domain-name\SYSVOL as a trusted directory (to allow execution of scripts).

Trusted User	Refers to an authorized Windows user with privileges to dynamically add to the whitelist. For example, add the administrator as a trusted user to allow the administrator to install or update any software. While adding the user details, you must also provide the domain details. Of all the strategies available to allow changes to protected endpoints, this is the least preferred because it offers minimal security. We suggest that you define trusted users judiciously because after a trusted user is added, there are no restrictions on what the user can modify or run on an endpoint.
Update mode	Refers to a time-window during which all changes are allowed on a protected endpoint. Place the protected endpoints in the Update mode to perform ad-hoc changes to the endpoints. Use this method when none of the other strategies, such as trusted users, trusted directories, publishers, or installers meet you requirements. For example, define a time window to allow the IT team to complete maintenance tasks, such as install patches or upgrade software. For more information on the Update mode, see the *Understanding Application Control modes* section.

Designing the trust model

Regardless of whether you use a rule group or policy, the framework available to define rules is the same. For more information on the type of rules you can define, see the *Managing protected endpoints* section.

Using variables in rules

The path specified in a rule can include system environment variables (only on the Windows platform). The following table lists the supported system variables.

Variable	Example value (true for most Windows platforms)
%ALLUSERSPROFILE%	C:\Documents and Settings\All Users
%APPDATA%	C:\Documents and Settings\{username}\Application
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C:
%HOMEPATH%	C:\Documents and Settings\{username}(\ on earlier Windows)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x*86)%	C:\Program Files (x86) (only in 64-bit version)
%SYSTEMDRIVE%	C:
%SYSTEMROOT%	C:\windows (C:\WINNT on earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:\Documents and Settings\{username}\local Settings\Temp C:\Temp
%USERPROFILE%	C:\Documents and Settings\{username} (C:WINNT\profiles\{username} for earlier versions)
%WINDIR%	C:\Windows

Understanding path considerations

These considerations apply to path-based rules.

- Path need not be absolute when specifying rules.

For example, when defining an updater you can specify the partial path, such as AcroRd32.exe or Reader\AcroRd32.exe or fully-qualified path, such as C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe. If you specify the partial path, all programs with names that match the specified string are assigned updater privileges. If you specify the fully-qualified path, only the specified program is assigned updater privileges.

Similarly, when banning a file if you specify the partial path, such as notepad.exe, all programs with names that match the specified string are banned. However, if you specify the fully-qualified path, for example C:\Windows\system32\notepad.exe, only the specified file is banned. Alternatively, if you specify the checksum value, only the file with the specified checksum value is banned.

- Paths can contain white spaces.
- Paths can include the wildcard character (*). However, it can only represent one complete path component. Here are a few examples.

Windows platform	Using \abc*\def is allowed while \abc*.doc, \abc*.*, or \abc\doc.* is not supported.
UNIX platform	Using /abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* is not supported.

Are any predefined rules available?

Yes, Application Control includes predefined rules for commonly-used applications. The following predefined rules are included:

- McAfee Default (one each for UNIX and Windows). For detailed information, see the *Reviewing the predefined rules* section.
- Common ActiveX Rules. For detailed information, see the *Reviewing predefined ActiveX rules* section.
- McAfee Applications (McAfee Default). This policy includes McAfee-specific rules that allow other McAfee products to run successfully on protected endpoints. These rules are also included in the McAfee Default (Windows) policy.

How do I define rules?

Use this table to define the rules to design the trust model. You can perform these actions when creating or modifying an Application Control policy or rule group.

Table 5: Designing the Trust Model

Action	Steps
Add an updater	1. Select the **Updaters** tab and click **Add**. The **Add Updater** dialog box appears. 2. Enter the location of the executable binary. 3. Specify an identification label for the program. For example, if you specify *Adobe Updater changes* as the label, all changes made by Adobe 8.0 updater are tagged with this label. 4. Specify conditions that the binary file must meet to run as an updater. • Select **None** to allow the binary file to run as an updater without any conditions. • Select **Parent** to allow the binary file to run as an updater only if it is launched by the specified parent. For example, when configuring updater.exe as an updater to allow changes to Mozilla Firefox, specify firefox.exe as the parent. Although updater.exe is a generic name that can be part of any installed application, using the parent ensures that only the correct program is allowed to run as an updater. • Select **Library** to allow the binary file to run as updater only when it has loaded the specified library. For example, when configuring iexplore.exe as an updater to allow Windows Updates using Internet Explorer, specify wuweb.dll as the library. This ensures that the iexplore.exe program has updater privileges only until the web control library (wuweb.dll) is loaded.

Action	Steps
	5. Indicate whether to disable inheritance for the updater. For example, if Process A (that is set as an updater) launches Process B, disabling inheritance for Process A ensures that Process B will not become an updater. 6. Indicate whether to suppress events generated for the actions performed by the updater. Typically, when a updater changes a protected file, a File Modified event is generated for the file. If you select this option, no events are generated for changes made by the updater. 7. Click **OK**.
Allow or ban a binary file	1. Select the **Binary** tab and click **Add**. The **Add Binary** dialog box appears. 2. Specify an identifier for the rule in the **Rule Name** field. You can use the identifier to group related rules. For example, you can specify *Banning unauthorized programs* as the identifier for all rules that you define to ban unauthorized programs in your organization. 3. Indicate whether to allow or ban the binary file. 4. Indicate whether to allow or ban the binary file based on the file's name or checksum value. 5. Enter the name or checksum value. 6. Click **OK**.
Specify authorized users permitted to override the protection in effect (only for the Windows platform)	You can either enter user details or import user or group details from an Active Directory. Ensure that the Active Directory is configured as a registered server. Specify details to authorize users to override the protection in effect . (Windows only) 1. Click **Add** on the **Trusted Users** tab. The **Add User** dialog box appears. 2. Enter the domain and logon name of the user in the domain\user format. 3. Specify a unique identification label for the user. For example, if you specify **John Doe's Changes** as the identification label for the John Doe user, all changes made by the user will be tagged with this label. 4. Type the user name. 5. Click **OK**.
	Import user details from an Active Directory. 1. Click **AD Import** on the **Trusted Users** tab. The **Import from Active Directory** dialog box appears. 2. Select the server. 3. Select **Global Catalog Search** to search for users in the catalog (only if the selected Active Directory is a Global Catalog server). 4. Specify whether to search for users based on the UPN (User Principal Name) or SAM account name. Note that your search will determine the authorized user. If you search using the UPN or common name, the user will be trusted with the UPN and if you search using the SAM account name, the user will be trusted with the SAM account name. 5. Enter the user name. The **Contains** search criteria is applied for the specified user name. 6. Specify a group name to search for users within a group. NOTE: You cannot directly add a group present in the Active Directory to a policy. To authorize all users in a group, add the user group to a rule group and include the rule group in a policy. Using groups ensures that all changes to a user group automatically cascade across all rule groups and associated policies. 7. Click **Find**. The search results are displayed. 8. Select the users to add in the search results and click **OK**.
Add a publisher	1. Select the **Publishers** tab and click **Add**. The **Add Publisher** dialog box appears. 2. Search for and add the certificate. For example, you can search for and add the Microsoft certificate. 3. Optionally, select the **Add Publisher(s) as Updater** option to provide updater privileges to the publisher. For example, if you set the Microsoft certificate that signs the Internet Explorer

Action	Steps
	application as an updater, Internet Explorer can download and execute any application from the internet. 4. Specify an identification label for the publisher. 5. Click **OK**.
Add an installer	1. Select the **Installers** tab and click **Add**. The **Add Installer** dialog box appears. 2. Search for and add the installer. For example, you can add the installer for the Adobe Reader to allow users to run the installer on the endpoints. 3. Specify an identification label for the installer. 3. Click **OK**.
Add an exception	1. Select the **Exceptions** tab and click **Add**. The **Add Attribute** dialog box appears. 2. Enter the file name. 3. Select the required options. For detailed information on the available options, see the *Defining memory-protection bypass rules* section. 4. Click **OK**.
Add a trusted directory	1. Select the **Trusted Directories** tab and click **Add**. The **Add Path** dialog box appears. 2. Enter the location of the directory. 3. Select **Include** or **Exclude**. Use the Exclude option to exclude a specific folder or subfolder within a trusted directory. 4. Optionally, select the **Make programs executed from this directory updaters** option to allow the software located at that UNC path to modify the endpoints. 5 Click **OK**.
Specify advanced exclusion filters	1. Click **Add Rule** on the Advanced tab. A new filter row appears. You can create filters based on files, events, programs, registry keys, and users. 2. Edit the settings to specify the filter. 3. Click **+** or **Add Rule** to specify additional AND or OR conditions, respectively. You can also define advanced exclusion filters from the **Events** page. For more information, see the *Excluding events* section.

Managing rule groups

As the name suggests, a rule group is a collection of rules. Although you can directly add rules to any McAfee ePO-based policy, the rules defined within a policy are specific to that policy. In contrast, a rule group is an independent unit that collates a set of similar or related rules. After you define a rule group, you can reuse the rules within the rule group by associating the rule group with different policies. Also, if you need to modify a rule, simply update the rule in the rule group and the change cascades across all associated policies automatically.

Application Control provides predefined rule groups to allow commonly-used applications to run smoothly. Although you cannot edit the predefined rule groups, you can use an existing rule group as a starting point to develop your rule groups. You can create a copy of an existing rule group and edit it to add more rules or create a new rule group. If needed, you can also import or export rule groups.

When do I use rule groups?

If you need to define similar rules across policies, using rule groups can drastically reduce the effort required to define rules. If you have a large setup and are deploying the software across

numerous endpoints, we recommend you use rule groups to minimize the deployment time and effort.

Consider an example. An organization runs Oracle on multiple servers. Each of these servers is used by the HR, Engineering, and Finance departments for different purposes. To reduce rule redundancy, we define an Application Control rule group (named AC-Oracle) containing rules to define the relevant updaters for Oracle to function.

After the rule group is defined, we can reuse these rule groups across policies for the HR, Engineering, and Finance departments. So, when defining the HR Servers policy, add the AC-Oracle rule group to the policy along with rule groups for the other applications installed on the HR server. Similarly, add the AC-Oracle rule group to the relevant policies for the Engg Servers and Fin Servers. After defining the policies, if you realize that the rule for a critical file was not created, directly update the rule group and all the policies will be updated automatically.

Contents

Creating a rule group

Use this task to create a rule group.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Solidcore Rules**.
2. Select **Application Control** from the **Rule Groups** tab.
   You can use an existing rule group as a starting point or define a new rule group from scratch. To modify an existing rule group, complete steps 3, 5, 6, and 7. To define a new rule group, complete steps 4, 5, 6, and 7.
3. Create a rule group based on an existing rule group.
   a. Click **Duplicate** for an existing rule group.
      The **Add Rule Group** dialog box appears.
   b. Specify the rule group name.
   c. Click **OK**.
      The rule group is created and listed on the **Rule Groups** page.
4. Define a new rule group.
   a. Click **Add Rule Group**.
      The **Add Rule Group** dialog box appears.
   b. Specify the rule group name.
   c. Select the rule group type and platform.
   d. Click **OK**.
      The rule group is created and listed on the **Rule Group**s page.
5. Click **Edit** for the rule group.
6. Specify the required rules.
   For information on the how to define rules, see the *Managing protected endpoints* and *Defining rules* sections.

7 Click **Save Rule Group**.

Importing or exporting a rule group

If you need to replicate the rule group configuration from one McAfee ePO server to another, export the rule group configuration from the (source) McAfee ePO server to an XML file and import the XML file to the (target) McAfee ePO server. You can also export rule groups into an XML file, edit the XML file to make the required changes to rule groups, and import the file to the McAfee ePO server use the changed rule groups.

Use this task to import or export rule groups.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Solidcore Rules**.

2 Complete one of these tasks from the **Rule Groups** tab.

- To import rule groups, click **Import**, browse and select the rule groups file, and click **OK**. While importing, you can specify whether to override rule groups (if you are importing a rule group with the same name as an existing rule group).
- To export selected rule groups to an XML file, select the rule groups, click **Export**, and save the file.

Viewing assignments for a rule group

Instead of navigating through all the created policies, you can directly view all the policies in which a rule group is being used. This feature provides a convenient way to verify if each rule group is assigned to the relevant policies.

Use this task to view the assignments for a rule group.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Solidcore Rules**.

2 Click **Assignments** on the Rule Groups tab for a rule group to view the policies to which the selected rule group is assigned.

Managing certificates

Add a certificate or publisher prior to defining rules to permit installation and execution of all software signed by the certificate. You can add a certificate regardless of the whether the certificate is an internal certificate or is issued to the vendor by a Certificate Authority.

NOTE: Application Control supports only X.509 certificates.

After you add a certificate and define it as a trusted publisher, all applications signed by the certificate are allowed. Also, all applications and binary files either added or modified on an endpoint that are signed by the certificate are automatically added to the whitelist.

Contents

Adding a certificate

You can use one of these methods to add a certificate.

- Upload an existing certificate available to you
- Immediately extract certificates from one or more signed binary files present on a network share
- Schedule a server task to routinely extract certificates from one or more signed binary files present on a network share

Use this task to add a certificate.

Task

For option definitions, click **?** in the interface.

1 Upload an available certificate by completing these steps.

a Select **Menu** | **Configuration** | **Solidcore Rules**.

b Switch to the **Publishers** tab.

c Select **Actions** | **Upload**.
The **Upload Certificate** page appears.

d Browse and select the certificate file to import.

e Click **OK**.

f Click **Upload**.

2 Extract certificates associated with one or more signed binary files present on a network share by completing these steps.

a Select **Menu** | **Configuration** | **Solidcore Rules**.

b Switch to the **Publishers** tab.

c Select **Actions** | **Extract Certificates**.
The **Extract Certificate from Binary** page appears.

d Type the path of the binary file.
Ensure that the file path is accessible from the McAfee ePO server.

e Specify the network credentials to access the specified network location.

f Click **Extract**.

3 Schedule and extract the certificates associated with one or more signed binary files present on a network share on a regular basis by completing these steps.

a Select **Menu** | **Automation** | **Server Tasks**.

b Click **New Task**.
The **Server Task Builder** wizard opens.

c Type the task name and click **Next**.

d Select **Solidcore: Scan a Software Repository** from the **Actions** drop-down list.

e Specify the repository path.
All subfolders in the specified path are also scanned for installers and publishers.

f Specify the network credentials to access the specified network location.

g Click **Test Connection** to ensure that the specified credentials work.

h Select **Add extracted certificates and installers to Rule Group** to add the certificates and installers extracted by the task to a user-defined rule group and select the user-defined rule group from the list.

NOTE: You can add extracted certificates and installers only to user-defined rule groups.

i Click **Next**.

j Specify the schedule for the task.

k Click **Next**.
The **Summary** page appears.

l Review the task summary and click **Save**.

If needed, you can specify an alias or friendly name for a certificate. Complete these steps to specify the friendly name for a certificate:

1 Select **Menu** | **Configuration** | **Solidcore Rules**.

2 Switch to the **Publishers** tab.

3 Select a certificate.

4 Click **Actions** | **Edit**.

The **Edit** window appears.

5 Enter the friendly name and click **OK**.

Assigning a certificate

After you add a certificate, you can assign it to a policy or rule group. Use this task to assign a certificate or publisher to a policy or rule group.

Task

For option definitions, click **?** in the interface.

1 Assign a certificate to a policy by defining a trusted publisher in an policy.
For more information, see the *Designing the trust model* and *Defining rules* sections.

2 Assign a certificate to an existing rule group.

a Select **Menu** | **Configuration** | **Solidcore Rules**.

b Switch to the **Publishers** tab.

c Select the certificates to add to a rule group.

d Click **Actions** | **Add to Rule Group**.
The **Add to Rule Group** dialog box appears.

e Select the user-defined rule group in which to add the certificates and click **OK**.

Alternatively, you can assign a certificate to a user-defined rule group by using the **Menu** | **Configuration** | **Solidcore Rules** | **Rule Groups** page. For more information, see the *Creating rule groups* section.

Searching for a certificate

Use this task to search for a certificate.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Solidcore Rules**.
2. Switch to the **Publishers** tab.
3. Select a category to sort the listed certificates.
   - **Issued to** — Sorts the list based on the name of the organization that publishes the certificate.
   - **Issued by** — Sorts the list based on the name of the signing authority.
   - **Extracted From** — Sorts the list based on the path of the binary file from which the certificate was extracted.
   - **Friendly Name** — Sorts the list based on the friendly name of the certificate.
4. Type the string to search for and click **Search**.

Viewing assignments for a certificate

This feature provides a convenient way to verify if each certificate is assigned to the relevant policies and rule groups.

Use this task to view assignments for a certificate.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Solidcore Rules**.
2. Switch to the **Publishers** tab.
3. Select a publisher and click **Actions** | **Check Assignments**.
   The **Publisher Assignments** dialog box lists the rule groups and policies to which the selected certificate is assigned.

Managing installers

Prior to defining rules to permit an installer to install or update software on endpoints, you must add the installer. You can add an executable binary or script file as an installer.

Contents

Adding an installer

You can use one of these methods to add an installer.

- Add an existing installer available to you
- Schedule a server task to routinely add installers

Use this task to add an installer.

Task

For option definitions, click **?** in the interface.

1 Add an existing installer by completing these steps.

a Select **Menu** | **Configuration** | **Solidcore Rules**.

b Switch to the **Installers** tab.

c Select **Actions** | **Add Installer**.
The **Add Installer** page appears.

d Enter the installer details.

e Click **Add**.

2 Schedule and add installers present on a network share on a regular basis by completing these steps.

a Select **Menu** | **Automation** | **Server Tasks**.

b Click **New Task**.
The **Server Task Builder** wizard opens.

c Type the task name and click **Next**.

d Select **Solidcore: Scan a Software Repository** from the **Actions** drop-down list.

e Specify the repository path.
All subfolders in the specified path are also scanned for installers and publishers.

f Specify the network credentials to access the specified network location.

g Click **Test Connection** to ensure that the specified credentials work.

h Select **Add extracted certificates and installers to Rule Group** to add the certificates and installers extracted by the task to a user-defined rule group and select the user-defined rule group from the list.

NOTE: You can add extracted certificates and installers only to user-defined rule groups.

i Click **Next**.

j Specify the schedule for the task.

k Click **Next**.
The **Summary** page appears.

l Review the task summary and click **Save**.

Assigning an installer

After you add an installer, you can assign it to a policy or rule group. Use this task to assign an installer to a policy or rule group.

Task

For option definitions, click **?** in the interface.

1. Assign an installer to a policy by defining a trusted installer in a policy.
   For more information, see the *Designing the trust model* and *Defining rules* sections.
2. Assign an installer to an existing rule group.
   a. Select **Menu** | **Configuration** | **Solidcore Rules**.
   b. Switch to the **Installers** tab.
   c. Select the installers to assign to a rule group.
   d. Click **Actions** | **Add to Rule Group**.
   The **Add to Rule Group** dialog box appears.
   e. Select the user-defined rule group in which to add the installers and click **OK**.

Alternatively, you can assign an installer to a user-defined rule group by using the **Menu** | **Configuration** | **Solidcore Rules** | **Rule Groups** page. For more information, see the *Creating rule groups* section.

Searching for an installer

Use this task to search for an installer.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Solidcore Rules**.
2. Switch to the **Installers** tab.
3. Select a category to sort the listed installers.
   - **Installer Name** — Sorts the list based on the name of the installer.
   - **Vendor** — Sorts the list based on the name of the vendor who published the installer.
4. Type the installer or vendor name to search for and click **Search**.

Viewing assignments for an installer

This feature provides a convenient way to verify if each installer is assigned to the relevant policies and rule groups.

Use this task to view assignments for an installer.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Solidcore Rules**.
2. Switch to the **Installers** tab.
3. Select an installer and click **Actions** | **Check Assignments**. The **Installer Assignments** dialog box lists the rule groups and policies to which the selected installer is assigned.

Deploying Application Control in Observe mode

Instead of directly placing endpoints in Enabled mode, you can place endpoints in Observe mode to perform a dry run for the Application Control product. When running in Observe mode, no action is blocked on the endpoints. Instead, an observation is logged corresponding to each action Application Control will take to protect an endpoint in Enabled mode. In effect, observations record all activity that occurs on the managed endpoints. For example, the installation of a software or modification of a package will generate corresponding observations.

Observations are generated every minute. All observations generated on an endpoint are sent to the McAfee ePO console after the agent-to-server-communication interval (ASCI) lapses. Note that when an endpoint is in Observe mode, no Application Control events are generated for the endpoint. To manage and analyze observations, you must review and take actions for the generated observations.

NOTE: Observe mode is available on all supported Windows platforms except Windows NT and Windows 2000. Note that Observe mode is not available on the UNIX platforms.

If you have multiple and different types of endpoints in your setup, we recommend you run Application Control in Observe mode only on a few endpoints. This will allow you to analyze product impact on each type of endpoint while ensuring no issues or breakage and discover relevant rules for your setup. You can also use the Observe mode to discover policy rules to run a new application prior to enterprise-wide deployment on endpoints already running Application Control. As you continue running the systems in Observe mode, you can analyze and take actions for the generated observations on a day-to-day basis.

Deploying Application Control in Observe mode involves the following high-level steps:

1. Identify the staging or test endpoints for deployment.
2. Place Application Control in Observe mode. For detailed information, see the *Placing the endpoints in Observe mode* section.
3. Run the endpoints with Application Control in Observe mode for a few days and perform day-to-day tasks on the endpoints.

   After the whiltelist is created, observations are generated for the endpoints allowing you to discover Application Control policy rules for the software installed on the endpoints.
4. Periodically review and take actions for the observations generated. This stage is referred to as rule discovery. In this stage, Application Control suggests adding appropriate updater, publisher, and other rules for relevant observations. For detailed information, see the *Managing Observations* section.
5. Create new or update existing rule groups based on the suggestions provided for the relevant observations.
6. Review generated observations to validate that no repeat observations are generated. As you process generated observations and add relevant rules in policies, the number of observations that are generated gradually declines. This stage is referred to as rule validation. If the appropriate rules are applied at the endpoints, repeat observations will not appear on the McAfee ePO console.

7 Exit Observe mode and place the endpoints in Enabled mode when the number of observations received reduces considerably. For detailed information, see the *Exiting Observe mode* section.

Contents

Placing the endpoints in Observe mode

After you complete installation, we recommend that you place selected endpoints (representing the different types of endpoints in your setup) in Observe mode by using the SC: Enable (Solidcore 6.0.0) client task. Place an existing endpoint (running in Enabled mode) in the Observe mode by using the SC: Observe mode (Solidcore 6.0.0) client task.

Use this task to place endpoints in Observe mode.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps from the McAfee ePO 4.6 console.

a Perform one of these actions.

- To apply the client task to a group, select the group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Client Task Assignment**.
The **Client Task Assignment Builder** page appears.

c Select the **Solidcore 6.0.0** | **SC: Enable** and click **Create New Task**.
The **Client Task Catalog** page appears.

d Specify the task name and add any descriptive information.

3 Complete these steps from the McAfee ePO 4.5 console.

a Perform one of these actions.

- To apply the client task to a group, select the group in the **System Tree** and switch to the **Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Task**.
The **Client Task Builder** page appears.

c Specify the task name and add any descriptive information.

d Select **SC: Enable (Solidcore 6.0.0)** and click **Next**.

The **Configuration** page appears.

4 Select the **Windows** platform.

5 Select the **All except NT/2000** subplatform.

6 Select the **6.0 and later** version.

7 Select the **Application Control** option.

8 Specify the scan priority.
The set scan priority determines the priority of the thread that is run to create the whitelist on the endpoints. We recommend you set the scan priority to **Low**. This ensures that Application Control causes minimal performance impact on the endpoints but might take longer (than when you set the priority to **High**) to create the whitelist.

9 Specify the activation option.

Limited Feature Activation	The endpoints are not restarted and limited features of Application Control (memory protection features are unavailable) are activated. Memory Protection features are available only after the endpoint is restarted.
Full Feature Activation	The endpoints are restarted, whitelist created, and all features of Application Control including Memory Protection are active. Restarting the endpoints is necessary to enable the memory protection features. The endpoint is restarted 5 minutes after the client task is received at the endpoint. A popup message is displayed on the endpoint before the endpoint is restarted.

10 Select the **Start Observe Mode** option.

11 Optionally, select the **Pull Inventory** option.
If you select this option, the inventory (including the created whitelist) is sent to McAfee ePO. We recommend that you select this option because inventory information is used in multiple workflows available from McAfee ePO.

12 Click **Save** (McAfee ePO 4.6 only).

13 Click **Next**.
The **Schedule** page appears.

14 Specify scheduling details and click **Next**.

15 Review and verify the task details and click **Save**.

16 Optionally, wake up the agent to send your client task to the endpoint immediately.

Understanding observations and suggestions

Observations record all activity for managed endpoints. The **Menu** | **Application Control** | **Observations** page on the McAfee ePO console is the central console for observations. Because Application Control groups related observations, this page displays only the collated observations.

How are observations grouped?

To keep the number of generated observations to a minimum level, after the observations are received from the endpoint, Application Control collates and groups related observations and only displays relevant observations. For example, if you try and install an application, such as googleTalk.exe on an endpoint, the installer spawns multiple child processes and each child process adds or updates files on the endpoint. In this scenario, Application Control will generate observations for all actions taken by the installer and its child processes. However, it will collate the observations generated for the installer (parent process) and its child processes and show

only relevant observations on the Observations page. For googleTalk.exe, all generated child observations will be collated in a parent observation where the object will be googleTalk.exe.

While collating observations, the software considers the identified Generic Launcher processes. Although observations are generated for Generic Launcher processes, no suggestions are provided. Note that while only relevant and collated observations are listed on the Observations page, suggestions are provided for all generated observations (including child observations).

Application Control uses heuristics to determine the actions listed for the each observation. The available actions are accurate for most cases; you might need to review the child observations in some cases. In most cases, taking actions for the most-relevant observation will do the needful. In some cases, in addition to taking actions for the relevant observation, you might need to review suggestions and take actions for the child observations.

What are Generic Launcher processes?

Certain processes on the Windows operating system, such as explorer.exe and iexplore.exe are launcher processes that are vital to the operating system. Such processes are referred to as Generic Launcher processes. A predefined list of such processes is available in Application Control. You can review and edit the list of Generic Launcher processes for which suggestions are not required.

1. Select **Menu** | **Configuration** | **Server Settings** | **Solidcore**.
2. Review the processes listed in the Observe Mode: Generic Launcher processes field.
3. Click **Edit**, add the process name to the end of this list (separated by a comma), and click **Save**.

How can I manage the observations?

When you open a collated observation from the Observations page, the Observations Detail page displays details for the selected observation. The Observations Detail page includes these components:

Binary Tree pane		Allows you to review information for all the child observations associated with the opened collated observation. By default, the file associated with the collated observation is selected in this pane. The tree hierarchically represents the relationship between the file and its parent process. It also lists all the child observations generated for the file. For information on the **Cloud Trust Score** and **Enterprise Trust Level** fields, see the *Interpreting the inventory* section.
Suggestions tab	Binary Info pane	Displays detailed information for the selected binary file and lists all the actions you can perform for the file.
	Publisher Info pane	Displays information for the certificate, if any, associated with the file. This pane is displayed only if a certificate is associated with the selected file.
	Rule Group pane	Displays the various rules to be added to the rule group. By default, this pane is empty and is populated based on the actions you perform.
	Files to be Whitelisted pane	Displays the various files to be whitelisted on the endpoint. By default, this pane is empty and is populated only when you choose the Add to Whitelist action.
Observations tab		Displays detailed information for observations in a tabular format.

How are suggestions provided for observations?

The following table details the various checks Application Control completes for each observation type. Please note the order in which the checks are performed for each observation type. If you are running in Observe mode with Full Feature Activation, all the listed observation types are generated. Because memory-protection features are not enabled in Limited Feature

Activation, the related observation types (Process Hijacked and Nx Violation Detected) are not generated if you are running Observe mode with Limited Feature Activation.

Also, in the Observe Mode, although observations are generated for Generic Launcher processes, no suggestions are provided. However, observations are generated and suggestions provided for processes spawned by the Generic Launcher processes.

Observation Type	Check Performed	Suggestion Provided
Execution Denied	1. Is the file a valid installer?	If yes, the **Add as Installer** action is displayed.
	2. Is the file stored on a network share or removable media?	If yes, the **Add as Trusted Directory** action is displayed. Note that the added trusted directory will be provided updater privileges.
	3. Is the file present in the whitelist?	If not, the **Add to Whitelist** action is displayed.
	4. Is the binary a Generic Launcher process?	If not, the **Add as Updater** action is displayed.
	5. Is the checksum value for the file available?	If yes, the **Add by Checksum** action is displayed.
	6. Is the file signed by a certificate?	If yes, the **Add Publisher** action is displayed. Note that adding the publisher will *NOT* provide updater privileges to the publisher.
File Write Denied	Is the parent process a Generic Launcher process?	If not, the **Add parent as Updater** action is displayed.
ActiveX Installation Prevented	The **Add Publisher** action is displayed.	
Process Hijack Attempted	Is the process a Generic Launcher process?	If not, the **Add as Exception** action is displayed.
Nx Violation Detected	Is the process a Generic Launcher process?	If not, the **Add as Exception** action is displayed.
Package Modification Prevented	1. Is the file stored on a network share or removable media?	If yes, the **Add as Trusted Directory** action is displayed. Note that the added trusted directory will be provided updater privileges.
	2. Is the file a valid installer?	If yes, the **Add as Installer** action is displayed.
Execution Denied/File Write Denied	1. The **Add as Updater** action is displayed.	
	2. Is the file signed by a certificate?	If yes, the **Add Publisher** action is displayed. Note that adding the publisher will *NOT* provide updater privileges to the publisher.

Managing observations

To manage observations:

1. Review the generated observations.
2. Analyze the suggestions available for the observations and approve or dismiss the observations. For more information, see the *Analyzing observations* section.
3. Optionally, delete processed observations to preserve database size. For more information, see the *Deleting observations* section.

Contents

Reviewing observations

Use this task to review the generated observations.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Application Control** | **Observations**.
   The **Solidcore Observations** page appears. On this page, you can review the following information for each observation:
   - Time at which the observation was logged
   - Name of the host on which the observation occurred
   - Name of user who caused the observation
   - Name and location of the object for which the observation was generated
   - Type of observation
   - Status of the observation (Approved, Dismissed, or Pending)
   - Remarks specified by the user while approving or dismissing the observation
   - Group to which the host belongs
2. Review selected observations by using one of these methods.
   - Select a time window, observation status, or both to view observations that match the filter criteria.
   - Enter a search string in the **Quick find** field and click **Apply** to view observations that match the specified search criteria.
   - Sort the list based on the time or object name by clicking the column heading.
   - Select the observations of interest and click **Show selected rows** to review only the selected observations.

To ignore or dismiss one or more observations, select the observations and click **Actions** | **Dismiss Observations**. Alternatively, you can review details for the observations and then choose to either approve or dismiss the observation. For more information, see the *Analyzing observations* section.

Analyzing observations

Use this task to analyze the suggestions available for an observation. You can choose to:

- Take actions based on the available suggestions and approve the observations.
- Dismiss irrelevant or routine observations and optionally define exclusion rules to stop receiving similar observations.

While approving or dismissing an observation, you can choose to approve and dismiss similar observations generated for other endpoints. Based on the observation type, all observations generated on different hosts with the same checksum value, file name, or ActiveX control name (whichever the case may be) are considered similar observations.

Task

For option definitions, click **?** in the interface.

1. Click **Show Suggestions**.
   Detailed information for the selected observation appears. By default, the file associated with the observation is selected in the **Binary Tree** pane.
2. View the file list in the **Binary Tree** pane.
   The tree hierarchically represents the relationship between the file and its parent process. It also lists all the observations generated for the file.
3. Analyze the suggestions available for the observation.
   a. Ensure that the relevant node is selected in the **Binary Tree** pane.
   b. Review the available suggestions.
   For all observations (except ActiveX Installation Prevented), the **Binary Info** pane is available on the **Suggestions** tab. The **Publisher Info** pane is displayed only if a certificate is associated with the file.

Binary Info	Displays detailed information for the binary file. You can review the binary name, path, checksum, Cloud Trust Score, and Enterprise Trust Level are displayed. For more information on these fields, see the *Interpreting the inventory* section. Depending on the file's properties and attributes, one or more of these actions are available for the file. • Add as Installer • Add as Updater • Add to Whitelist • Add Parent as Updater • Add as Exception • Add by Checksum • Add as Trusted Directory NOTE: The **Add to Whitelist** action differs from the other actions available for the file. When you select the **Add to Whitelist** action, a task is created and applied to the specific endpoint. Selecting any other action, such as **Add by Checksum** allows you to add rules to a specific rule group that can be included in one or more policies.
Publisher Info	Displays information for the certificate associated with the file. For the certificate you can review these details: • Company name the certificate is issued to • Certificate issuing authority • Expiry date for the certificate • Friendly name for the certificate For a certificate, you can click **Add Publisher** to add the certificate as a trusted publisher.

c Review the order in which the suggestions are listed.
The suggestions order indicates the preferred and suitable actions to take for the observation.

d Review the cloud trust score and trust level for the file.
This will help you easily identify malicious files and malware.

You can choose to either take actions and approve the observation (perform step 4) or dismiss the observation (perform step 5).

4 Approve the observation.

a Take the required actions for the file. For detailed information on each action, see the *Managing protected endpoints* section.
The **Rule Group** and **Files to be Whitelisted** panes are updated based on the selected actions.

b Review the information in the **Rule Group** and **Files to be Whitelisted** panes.
While all the rules listed in the **Rule Group** pane are added to a rule group (and impact all polices that include the rule group), the files listed in the **Files to be Whitelisted** pane are added to a task that is applied to the endpoint. Note that the **Add to Whitelist** action does not result in the any rule group or policy changes.

c Specify the rule group for the rules.

- To add the rules to an existing rule group, select **Add to an existing Rule Group** and select the rule group from the list.
- To create a new rule group with the rules, select **Create a new Rule Group** and enter the rule group name.

d Click **Approve**.
The **Approve** window appears.

e Enter remarks to optionally provide a description for the approval.

f Select **Approve Similar Observations** to approve similar observations on other endpoints.

g Click **OK**.

h Ensure the updated rule group is included in a policy applied to the endpoint.

5 Dismiss the observation.

a Click **Dismiss**.
The **Dismiss** window appears.

b Enter remarks to optionally specify the reason for dismissing.
You can choose to perform these actions:

- Ignore selected observations and set their status to Dismissed (perform only step e)
- Ignore selected observations and other similar observations and set their status to Dismissed (perform steps c and e)
- Ignore selected observations, set their status to Dismissed, and define exclusion rules to ensure the observations do not appear on the **Observations** page in future (perform steps d and e)
- Ignore selected observations and other similar observations, set their status to Dismissed, and define exclusion rules to ensure the observations do not appear on the **Observations** page in future (perform steps c, d, and e)

c Select **Dismiss Similar Observations** to ignore similar observations on other endpoints.

d Select **Create Exclusion Rules** to define exclusion rules for the selected observations.

You can define rules to prune routine or system-generated observations not relevant for monitoring or auditing.

e Click **OK**.

Deleting observations

Use this task to delete observations. Note that deleting the observations removes the selected observations from the Observations page and the database.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Application Control** | **Observations**.
   The **Solidcore Observations** page displays all observations.
2. Select the observations to delete.
3. Click **Actions** | **Delete Observations**.
   The **Delete Observations** window appears.
4. Optionally, select **Delete Similar Observations** to delete similar observations.
   All observations with the same checksum or file name on different hosts are considered similar observations.
5. Click **OK**.

Reviewing exclusion rules

Use this task to view and manage the defined exclusion rules.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Application Control** | **Observations**.
   The **Solidcore Observations** page displays all observations.
2. Click **Show Exclusion Rules**.
   The **Solidcore Observations Exclusion Rules** page displays all exclusion rules.
3. Review the listed rules.
4. Optionally, delete the exclusion rules.
   a Select the rules to delete.
   b Click **Actions** | **Delete**.
5. Click **Close**.

Exiting Observe mode

Use this task to exit Observe mode and switch to Enabled mode.

Before you begin

Ensure the number of observations you receive on a day-to-day basis are negligible.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Systems** | **System Tree**.
2. Complete these steps from the McAfee ePO 4.6 console.
   a. Perform one of these actions.
      - To apply the client task to a group, select the group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
      - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b. Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.

   c. Select the **Solidcore 6.0.0** | **SC: Observe Mode** and click **Create New Task**.
   The **Client Task Catalog** page appears.

   d. Specify the task name and add any descriptive information.
3. Complete these steps from the McAfee ePO 4.5 console.
   a. Perform one of these actions.
      - To apply the client task to a group, select the group in the **System Tree** and switch to the **Client Tasks** tab.
      - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b. Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c. Specify the task name and add any descriptive information.

   d. Select **SC: Observe Mode (Solidcore 6.0.0)** and click **Next**.
   The **Configuration** page appears.
4. Select **End Observe Mode**.
5. Specify whether to place the endpoints in Enabled or Disabled mode.
6. Indicate whether to update the whitelist based on the changes made in Observe mode.
   If you have modified existing files on the endpoint running in Observe mode, make sure you update the whitelist based on changes made to the endpoint.
7. Click **Save** (McAfee ePO 4.6 only).
8. Click **Next**.
   The **Schedule** page appears.
9. Specify scheduling details and click **Next**.
10. Review and verify the task details and click **Save**.
11. Optionally, wake up the agent to send your client task to the endpoint immediately.

Monitoring your protection

When Application Control is running in Enabled mode, only authorized programs can run (executable binary and script files), unauthorized programs cannot run, and authorized programs cannot be changed. Application Control provides various methods to allow changes to the managed endpoints while in Enabled mode. You can choose to define updaters, publishers, installers, trusted users, and trusted directories. Also, to perform ad-hoc changes to the endpoints, you can place the endpoints in Update mode. For detailed information on each method, see the *Managing protected endpoints* section.

Contents

Enabling Application Control

Use this task to activate the Application Control software.

NOTE: If the endpoints are running in Observe mode, we recommend you use the **SC: Observe Mode** client task to exit Observe mode and place the endpoints in Enabled mode. For detailed instructions, see the *Exiting Observe mode* section.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps from the McAfee ePO 4.6 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the Systems page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Client Task Assignment**.
The **Client Task Assignment Builder** page appears.

c Select the **Solidcore 6.0.0** | **SC: Enable** and click **Create New Task**.
The **Client Task Catalog** page appears.

d Specify the task name and add any descriptive information.

3 Complete these steps from the McAfee ePO 4.5 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the Systems page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c Specify the task name and add any descriptive information.

   d Select **SC: Enable (Solidcore 6.0.0)** and click **Next**
   The **Configuration** page appears.

4 Select the platform.

5 Select the subplatform (only for the Windows and UNIX platforms).

6 Select the version (only for the All except NT/2000 subplatform).

7 Select the **Application Control** option.

8 Complete these steps to enable Application Control if you are using Solidcore client version 6.0.0 or later on the supported Windows platforms. Note that Solidcore client version 6.0 is not available for the Windows NT, Windows 2000, Linux, Solaris, and WindRiver Linux platforms.

   a Specify the scan priority.
   The set scan priority determines the priority of the thread that is run to create the whitelist on the endpoints. We recommend you set the scan priority to **Low**. This ensures that Application Control causes minimal performance impact on the endpoints but might take longer (than when you set the priority to **High**) to create the whitelist.

   b Specify the activation option.

Limited Feature Activation	The endpoints are not restarted and limited features of Application Control (memory protection features are unavailable) are activated. Memory Protection features are available only after the endpoint is restarted.
Full Feature Activation	The endpoints are restarted, whitelist created, and all features of Application Control including Memory Protection are active. Restarting the endpoints is necessary to enable the memory protection features. The endpoint is restarted 5 minutes after the client task is received at the endpoint. A popup message is displayed on the endpoint before the endpoint is restarted.

   c Select the **Start Observe Mode** option to place the endpoints in Observe mode.

   d Optionally, select the **Pull Inventory** option.
   If you select this option, the software fetches the inventory details for the endpoints (after the whitelist is created) and makes the details available on the McAfee ePO console when the agent-to-server-communication interval (ASCI) lapses. We recommend you select this option if you wish to manage the inventory using the McAfee ePO console.

9 Complete these steps if you are using the Solidcore client version 5.1.5 or earlier.

   a Select the **Perform Initial Scan to create whitelist** option to create the whitelist when enabling Application Control.
   Application Control requires the creation of a list of all trusted executable files present on the endpoint system (known as the whitelist). The one-time activity of creating the

whitelist is known as whitelisting or solidification. You can choose to create the inventory while enabling the Solidcore client or defer it to later.

NOTE: If you defer the scan, run the **SC: Initial Scan to create whitelist** client task after the **SC: Enable** task is applied and system is restarted.

b Select **Force Reboot with the task** to restart the endpoint after solidification is complete.
Restarting the system is necessary to enable the software. A popup message is displayed at the endpoint 5 minutes before the endpoint is restarted. This allows the user to save work and data on the endpoint.

10 Click **Save** (McAfee ePO 4.6 only).

11 Click **Next**.
The **Schedule** page appears.

12 Specify scheduling details and click **Next**.

13 Review and verify the task details and click **Save**.

14 Optionally, wake up the agent to send your client task to the endpoint immediately.

Reviewing predefined rules

Application Control includes predefined rules to allow multiple commonly-used applications, such as Oracle and Adobe Acrobat to run. By default, these rules are applied to the global root in the system tree and hence are inherited by all McAfee ePO-managed endpoints. As soon as an endpoint connects to the McAfee ePO, the McAfee Default policy applicable to the endpoint's operating system comes into play.

Use this task to review the predefined rules included in the McAfee Default policy.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Policy** | **Policy Catalog**.

2 Select the **Solidcore 6.0.0: Application Control** product.
All policies for all categories are listed. Note that a **McAfee Default** policy exists for each supported operating system.

3 Open the relevant policy.

4 Review the rules.

5 Click **Cancel**.

Reviewing events

Any action to change or execute a file or program on a protected system causes Application Control to prevent the action and generate a corresponding event on the endpoint. All generated events for managed systems are sent to the McAfee ePO server. Review and manage the generated events to monitor the status of the managed endpoints.

Use this task to review and manage the events from the McAfee ePO console.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting** | **Solidcore Events**.
2. Specify the time duration for which to view events by selecting an option from the **Time Filter** list.
3. Specify the endpoints for which to view events.
   a. Select the required group in the **System Tree**.
   b. Select an option from the **System Tree Filter** list.
4. Optionally, view only specific events by applying one or more filters.
   a. Click **Advanced Filters**.
   The **Edit Filter Criteria** page appears.
   b. Select an available property.
   c. Specify the comparison and value for the property.
   For example, to view only Execution Denied events, select the Event Display Name property, set comparison to Equals, and select the Execution Denied value.
   d. Click **Update Filter**.
   Events matching the specified criteria are displayed.
5. View details for an event by clicking the corresponding row.
6. Review endpoint details for one or more events.
   a. Select one or more events.
   b. Click **Actions** | **Show Related Systems**.
   The **Related Systems** page lists the endpoints corresponding to the selected events.
   c. Click a row to review detailed information for the endpoint.
   d. Optionally, perform any action on the endpoint.

Defining rules

Use one of these methods to define rules to allow changes and override the applied protection:

- Review suggestions and take actions available for events. For detailed instructions, see the *Reviewing suggestions* section.
- Add specific rules to a rule group or policy. For detailed instructions, see the *Creating a policy* section.
- Apply exclusion rules to prune routinely generated events. For detailed instructions, see the *Excluding events* section.
- Define specific rules in a policy to bypass applied memory-protection techniques. For detailed instructions, see the *Defining memory-protection bypass rules* section.

Contents

Reviewing suggestions

For most events, you do not need to take any actions. However, if the protection that is in effect is preventing a legitimate application from executing, you will need to define rules. To allow you to define rules with ease, Application Control generates events and corresponding observations for these events:

- Execution Denied
- File Write Denied
- Process Hijack Attempted
- Nx Violation Detected
- ActiveX installation Prevented
- Package Modification Prevented

Use this task to review suggestions available for the generated events and take actions based on the available suggestions.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting** | **Solidcore Events**.
2. Specify the time duration for which to view events by selecting an option from the **Time Filter** list.
3. Specify the endpoints for which to view events.
   a. Select the required group in the **System Tree**.
   b. Select an option from the **System Tree Filter** list.
4. Click **Show Suggestions**.
   Detailed information for the selected event appears.
5. Approve or dismiss the observation corresponding to the suggestions.
   For more information, see the *Analyzing observations* section.
6. Ensure the updated rule group is included in a policy applied to the endpoint.

Creating a policy

Use this task to add specific rules to a rule group or policy. Note that Application Control policies are multi-slot policies; a user can assign multiple policies to a single node in the system tree.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. Select the **Solidcore 6.0.0: Application Control** product.
3. Click **Actions** | **New Policy**.
   The **New Policy** dialog box appears.
4. Select the category.
5. Select the policy you want to duplicate from **Create a policy based on this existing policy** list.
   To define a policy from scratch, select the **Blank Template** policy.
6. Specify the policy name and click **OK**.

The **Policy Settings** page opens. You can now define the rules to include in the policy. You can either add the rules to a rule group or directly add the new rules to the policy.

- To use a rule group, complete steps 7 and 9. For more information on how to create a rule group, see the *Creating rule groups* section.
- To directly add the rules to the policy, complete steps 8 and 9.

7 Add a rule group to the policy.

a Select the rule group in the **Rule Groups** tab.
The rules included in the rule group are displayed in the various tabs.

b Review the rules.
For more information on adding new rules to the rule group, see the *Managing rule groups* section.

c Select **Add** in the **Rule Groups** tab.
The **Select Rule Groups** dialog box appears.

d Select the rule group to add.

e Click **OK**.

8 Add the rules to the policy.
For information on the rules, see the *Designing the trust model* section.

9 Save the policy.

Excluding events

You can define rules to prune routine system-generated events not relevant for monitoring or auditing. Use this task to exclude or ignore events not required to meet compliance requirements.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Reporting** | **Solidcore Events**.

2 Select the events to exclude.

3 Click **Actions** | **Exclude Events**.
The **Events Exclusion** wizard appears.

4 Select the target platform for the rules.

5 Select the rule group type and click **Next**.
The **Define Rules** page appears.

6 Rules are auto-populated based on the selected events.

7 Review and refine existing rules and add new rules, as needed.

8 Click **Next**.
The **Select Rule Group** page appears.

9 Add the rule to an existing or new rule group and click **Save**.

10 Ensure the rule group is added to the relevant policy and the policy is assigned to the endpoints.

Defining memory-protection bypass rules

Application Control provides these memory-protection techniques.

• Critical Address Space Protection (CASP) • Data Execution Protection (DEP)	CASP and DEP are a memory-protection techniques that prevent all code running from the non-executable memory region. In most cases, code running from the non-executable memory region is an abnormal event. This mostly occurs when a buffer overflow happens. CASP is available on 32-bit Windows platforms and DEP is available on 64-bit Windows platforms.
Call Context Verification (CCV)	CCV checks that the critical Kernel32 API calls are made from a code page region that belongs to a loaded module. In addition, we try to ascertain that the APIs are being made through a call instruction and not as a result of a jump or return from a routine. This feature is available on 64-bit Windows platforms only.
Address Space Layout Randomization (ASLR)	ASLR randomizes the addresses where modules are loaded to help prevent an attacker from leveraging data from predictable locations. The problem with this is that all modules have to use a compile time flag to opt into this. With Forced ASLR in place, we force modules to be loaded at randomized addresses for a target process regardless of the flags it was compiled with. Exploits using return-oriented programming (ROP) and relying on predictable mappings will fail. This feature is available on 64-bit Windows platforms only.
Process Context File Operations Bypass	In certain scenarios, Application Control can prevent legitimate applications from running. In such cases, you can define a bypass rule for the application (on 32-bit and 64-bit Windows platforms) by using the **Process Context File Operations Bypass** option. Use this option judiciously because it may impact default Application Control functionality.

NOTE: Contact McAfee Support for information on other deprecated memory-protection techniques, such as API Mangling, Decoying, and Virtual Address Space Randomization (VASR).

Some applications (as part of their day-to-day processing) run code in an atypical way and hence are prevented from running. To allow such applications to run, define appropriate bypass rules. Note that a bypassed file or application is no longer considered by the memory-protection features of Application Control. Bypassing a file should be the last-resort to allow an application to run and should be used judiciously.

Use this task to override or bypass the applied memory-protection techniques.

Task

For option definitions, click **?** in the interface.

1. Perform one of these tasks.
   - Define a new Application Control rule group (to define bypass rules to reuse across multiple endpoints). For detailed instructions, see the *Creating a policy* section.
   - Create a new Application Control policy (to apply bypass rules to a single endpoint). For detailed instructions, see the *Creating a rule group* section.
2. Select the **Exceptions** tab.
3. Click **Add**. The **Add Attribute** window appears.
4. Enter the file name.
5. Select the required options.
6. Optionally, for the **Process Context File Operations Bypass** or **Bypassed from ASLR** options, specify the parent to allow the file to bypass the memory-protection feature only if it is launched by the specified parent.
7. Click **OK**.

Allowing ActiveX controls to run

By default, Application Control prevents the installation of ActiveX controls on endpoints. You can use the ActiveX feature to install and run ActiveX controls on endpoints. This feature is enabled by default and available only on the Windows platform.

NOTE: Only the Internet Explorer browser is supported for ActiveX control installations. If you are using a 64-bit operating system, installation of ActiveX controls is supported only for the 32-bit Internet Explorer application. Simultaneous installation of ActiveX controls using multiple tabs of Internet Explorer is not supported.

Here are high-level steps to help you use the ActiveX feature.

1. Apply the **Common ActiveX Rules** policy to the endpoints to allow users to install commonly-used ActiveX controls on the endpoints.
2. Perform one of these tasks.
   - If the ActiveX control you need to install is listed in the predefined rules, you can directly install the ActiveX control (complete step 3).
   - If the ActiveX control you need to install is not listed in the predefined rules, Application Control prevents the installation of the ActiveX control on the endpoint and generates the ActiveX Installation Prevented event. (complete steps 3, 4, and 5)
3. Install the required ActiveX control on the endpoint.
4. Review and take actions for ActiveX Installation Prevented event. Click **Add Publisher** to add the certificate associated with the ActiveX control as a trusted publisher. For detailed information, see the *Reviewing suggestions* section.
5. Ensure the updated rule group is included in a policy applied to the endpoint.

Managing the inventory

You can fetch, review, and manage the software inventory for protected endpoints. The software inventory for an endpoint contains information about the executable binary and script files present on the endpoint. The information stored in the inventory includes complete file name, file size, checksum, file type, embedded application name, version, and so on. The software inventory for an endpoint can be fetched and managed via the McAfee ePO console. You can perform multiple tasks, such as allow or ban specific binary files, review all the occurrences of an application or binary file in the enterprise, and compare the endpoint inventory with a gold system to view image deviation.

Contents

Fetching the inventory

Application Control provides multiple methods to help you fetch the software inventory for an endpoint.

1. Use the Enable client task to fetch the inventory for endpoints when you place the endpoints in Enabled mode. For more information, see the *Enabling Application Control* section.
2. Use the Fetch Inventory link on the **Menu** | **Application Control** | **Inventory** | **Inventory By Systems** page to fetch the inventory for selected endpoints.
3. Use the Fetch Inventory action for a selected endpoint on the **Menu** | **Systems** | **System Tree** | **Systems** page to fetch the inventory for an endpoint.
4. Using the Pull Inventory client task you can fetch the inventory for one or more endpoints.

NOTE: Application Control also allows you to import inventory details for endpoints not connected to the McAfee ePO console. Execute the sadmin ls -lax > <XML file name> command on the endpoint using the CLI to generate an XML file with inventory details. On the McAfee ePO console, select the endpoint on the **Menu** | **Systems** | **System Tree** | **Systems** page and click **Actions** | **Import Inventory**. The inventory for the selected endpoint is updated based on the inventory details included in the XML file.

Use the Enable client task, Fetch Inventory link, and Fetch Inventory action to quickly fetch inventory for an endpoint. We recommend you use the Pull Inventory to fetch inventory details for a group. Use this task to fetch the software inventory for one or more endpoints.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.
2 Complete these steps for the McAfee ePO 4.6 console.
   a Perform one of these actions.
      • To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
      • To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.
   b Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.
   c Select the **Solidcore 6.0.0** product, **SC: Pull Inventory** task type, and click **Create New Task**.
   The **Client Task Catalog** page appears.
   d Specify the task name and add any descriptive information.
3 Complete these steps for the McAfee ePO 4.5 console.
   a Perform one of these actions.
      • To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
      • To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.
   b Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.
   c Specify the task name and add any descriptive information.
   d Select **SC: Pull Inventory (Solidcore 6.0.0)** and click **Next**.
   The **Configuration** page appears.
4 Click **Save** (McAfee ePO 4.6 only).
5 Click **Next**.
   The **Schedule** page appears.
6 Specify schedule details and click **Next**.
7 Review and verify the task details and click **Save**.
8 Optionally, wake up the agent to send your client task to the endpoint immediately.

Interpreting the inventory

Application Control is integrated with the McAfee GTI file reputation service. The software synchronizes with the GTI file reputation service on a regular basis to fetch information. If Application Control finds a new SHA1 in the enterprise, it immediately fetches information for the SHA1 from the GTI file reputation service. For existing files, Application Control fetches information as soon as the time to live (TTL) value (set by GTI file reputation service) expires for a file. Here are the TTL values assigned to each trust score by the GTI file reputation service.

Trust score	TTL value
1	1 day
2	2 days
3	5 days

Trust score	TTL value
4 or 5	30 days

For each binary file, GTI provides these values:

Cloud Trust Level

Indicates if the file is a good, bad, or unknown file. Based on information fetched from GTI, the application and binary files in the inventory are sorted into Good, Bad, and Unclassified categories.

For every Bad binary file encountered in your setup, the software generates the **Bad File Found** event. Also, if the trust level for a binary file changes from Bad to Good, the **Assumed Bad File is Clean** event is generated. You can view these events on the **Menu** | **Reporting** | **Threat Event Log** page. If needed, you can set up responses to receive a notification for these events.

Cloud Trust Score

Indicates the reliability or credibility of the file. The assigned value ranges between 1 to 5. A value of 1 or 2 represents known bad files, such as trojan, virus, and Potentially unwanted programs (PUP) files. A value of 3 indicates an Unclassified file. A value between 4 or 5 represents known and trusted good files.

Value	Description	Details
5	Known Clean	Represents files that belong to known, trusted software vendors that McAfee considers clean due to the analysis and reputation of the file, application, software vendor, or digital signature.
4	Assumed Clean	Indicates a high probability that these files are clean based on McAfee's heuristic analysis computed from file reputation and telemetry data.
3	Unknown	Indicates that McAfee did not have sufficient data on these files to conclusively categorize the files as good or bad.
2	Suspicious	Indicates that the files are suspicious and maybe malware (based on McAfee's heuristic and behavioral analysis computed from file reputation, telemetry data, and emulation).
1	Malicious	Indicates that the files have been analyzed and determined to be malware.

In addition to the above values, Application Control also tracks the **Enterprise Trust Level** value for each binary file. By default, the enterprise trust level for a file is the same as the cloud trust level. When edited, the enterprise trust level for a file overrides the cloud trust level for the file.

For example, if your organization uses an internally-developed application, GTI will mark it as an Unclassified application because it is specific to your organization. However, because you trust the application, you can recategorize it as a Good file by editing the enterprise trust level for the file. To edit the enterprise trust level for a file, select the file and select **Actions** | **Change Enterprise Trust Level**.

Reviewing the inventory

Use this task to manage and take actions on the software inventory for an endpoint.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Application Control** | **Inventory**.
2. Perform one of these tasks.
   - To manage the inventory for all managed endpoints, select the **Inventory By Applications** tab.
   - To manage the inventory for a selected endpoint, switch to the **Inventory By Systems** tab and click **View Inventory** for the relevant endpoint.

   The inventory for the selected endpoint is listed.

3 Review the applications in the inventory. By default, based on information received from GTI, the application and binary files are sorted into Good, Bad, and Unclassified categories. Here are some alternate views you can use.

Review all binary files	• To view files sorted by name, select **Binary Name** filter, leave the filter blank, and click **Search**. • To view files sorted by checksum, select **Binary SHA1** filter, leave the filter blank, and click **Search**.
Review all files sorted by applications	Select **Application** filter, leave the file name filter blank, and click **Search**. The applications and binary files are sorted into Good, Bad, and Unclassified categories.
Sort the application and binary files based on vendor	Select the **Vendor** filter, do not specify a vendor name, and click **Search**. The applications and binary files are sorted by the vendor. For each vendor, you can view the Good, Bad, and Unclassified categories.

4 Review application details (only when you review all files sorted by applications).

a Click **App Details**.
The **Application Details** page appears.

b View the details for the application.

c Review the binary files associated with the selected application in the **Binaries** pane.

d Review the endpoints on which the selected application is present in the **Systems** pane.

e Optionally, perform any action on the listed endpoints.

f Click **Close**.

5 Optionally, apply seeded filters, create new filters, or search for specific files, as needed.

Use seeded filters	Select a value from the **Saved Filters** list. You can choose from these filters: • All Ban Binaries • Allowed Bad Binaries • Allowed Unclassified Signed Binaries • Allowed Unclassified Unsigned Binaries • Banned Good Binaries
Create a new filter	To create a new filter: 1. Select the **Add Saved Filter** option from the Saved Filters list. 2. Select an available property. For example, to identify all unclassified applications that are signed, select the **Has Cert** and **Trust Level (Enterprise)** properties. 3. Specify the comparison and value for the property. • For the **Has Cert** property, set comparison to **Equals**, and select the **True** value. • For the **Trust Level (Enterprise)** property , set comparison to **Equals**, and select the **Unclassified** value. 4. Click **Update Filter**.
Search for specific files, for example search for a file based on its checksum value	Select the **Binary SHA1** filter, enter a checksum value, and click **Search**. The binary file with the specified checksum value is displayed.

6 Review the binary files.
When you view files sorted by applications or vendors, the **Applications** or **Vendors** pane is displayed. The pane provides a tree structure to help you navigate and view the files under each category. Select a node in the tree to review associated binary files in the **Binaries** pane. For all other views, only the **Binaries** pane is displayed. For each file, the

Binaries pane lists the name, version, trust score, trust level (cloud and enterprise), allowed system count, and banned system count.

7 View binary details.

a Click a binary file.
The **Binary Details** page appears.

b Click the cloud trust score to view the details fetched from the GTI server for the binary file.

c Review the endpoints listed in the **System for this Binary** pane.

d Click **View Events** for an endpoint to view events generated for the endpoint.

e Click **Ban** to ban the binary file from an endpoint.

f Click **Close**.

Managing the inventory

Application Control sorts your inventory files into these categories:

Good	Includes known good or trusted applications (effectively creating the Whitelist for your enterprise). Because these applications are known files, you do not need to perform extensive management activities for the good files. If your organization needs to disallow a known good file, you can ban the file.
Bad	Includes known malware or bad applications (effectively creating the Blacklist for your enterprise). Because these applications are known bad files, for the most part, you will need to ban the bad applications. If needed, you can categorize any in-house or trusted applications in the bad list as a good file.
Unclassified	Includes all unknown applications (effectively creating the Graylist for your enterprise). You should routinely review and manage the graylist for your enterprise to keep it to a minimum size (ideally zero). You might need to reclassify internally developed, recognized, or trusted (from a reputed vendor) files that are currently in the unclassified list. NOTE: Any pre-existing advanced persistent threat (APTs) will reside in the Graylist or Unclassified category.

Use this task to manage the files in the inventory.

Task

For option definitions, click **?** in the interface.

1 Perform one of these tasks.

- To manage the inventory for all managed endpoints, navigate to the **Menu** | **Application Control** | **Inventory** | **Inventory By Applications** page.
- To manage the inventory for a selected endpoint, navigate to the **Menu** | **Application Control** | **Inventory** | **Inventory By Systems** page and click **View Inventory** for the relevant endpoint.

2 Prevent bad binary or script files from running.

a Select the files to ban.

b Select **Actions** | **Ban Binaries**.
The **Allow or Ban Binaries** wizard appears.

c Specify the rule group for the rules.

- To add the rules to an existing rule group, select **Add to Existing Rule Group**, select the rule group from the list, and specify the operating system.

- To create a new rule group with the rules, select **Create a New Rule Group**, enter the rule group name, and specify the operating system.

d Click **Next**.

e Review the rules and click **Save**.

3 Allow known binary or script files to run.

a Select the files to allow.

b Select **Actions** | **Allow Binaries**.
The **Allow or Ban Binaries** wizard appears.

c Perform one of these tasks.

- To allow the binary file only on the selected endpoint, add the binary file to the whitelist of the endpoint by selecting the **Add Binaries to Whitelist** option. This option is available only if when you are managing the inventory for an endpoint (by clicking the **View Inventory** link for an endpoint on the **Inventory By Systems** page).
- To allow the binary file on multiple endpoints, to add the rules to a rule group.

Add the rules to an existing rule group	Select **Add to Existing Rule Group**, select the rule group from the list, and specify the operating system.
Create a new rule group with the rules	Select **Create a New Rule Group**, enter the rule group name, and specify the operating system.

d Click **Next**.

e Review the rules and click **Save**.

4 Recategorize an unclassified binary or script file as a good file by editing the enterprise trust level for the file.

a Select the files.

b Select **Actions** | **Change Enterprise Trust Level**.
The **Change Enterprise Trust Level** window appears.

c Set the trust level.
By default, the enterprise trust level for a file is the same as the cloud trust level. When edited, the enterprise trust level for a file overrides the cloud trust level for the file.

5 Add the updated rule group to the policies applied to the endpoints.

Comparing the inventory

Image deviation is used to compare the inventory of an endpoint with the inventory that is fetched from a designated gold system. This helps you to track the inventory present on an endpoint and identify any differences that occur. To accomplish this, complete these steps.

1 Fetch the inventory for your gold host. For detailed information, see the *Fetching the inventory* section.

2 Fetch the inventory for the endpoint. For detailed information, see the *Fetching the inventory* section.

3 Review the **Menu** | **Automation** | **Solidcore Client Task Log** page to ensure that both client tasks completed successfully.

4 Compare the inventory of gold host with the inventory of the endpoint. This is known as Image Deviation.

5 Review the comparison results.

Contents

Running the inventory comparison

Use this task to compare the inventory of the gold host with the inventory of an endpoint.

Before you begin

Ensure that you have recently fetched the inventory for the gold host and endpoint.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Automation** | **Server Tasks**.

2 Click **New Task**.
The **Server Task Builder** wizard opens.

3 Type the task name and click **Next**.

4 Select **Solidcore: Run Image Deviation** from the **Actions** drop-down list.

5 Specify the gold system.

6 Configure these options to select the endpoint to compare with the gold system.

- **System to compare with Gold System** — Click **Add** to search for the endpoint that you want to compare with the gold system. Type the name of the endpoint in the **System Name** field and click **Search**.
- **Groups to compare with Gold System** — Click **Add** to search for the group that you want to compare with the gold system. Type the name of the group in the **Group Name** field and click **Search**.
- **Include Systems with Tags** — Click **Add** to search for endpoints based on their tag names. Type the tag name in the **Tag Name** field and click **Search**.
- **Exclude Systems with Tags** — Click **Add** to search for endpoints based on their tag names. Type the tag name in the **Tag Name** field and click **Search**. Select the required tag from the search result. All endpoints with the selected tags are excluded from comparison with the gold system.

7 Click **Next**.
The **Schedule** page appears.

8 Specify the schedule for the task.

9 Click **Next**.
The **Summary** page appears.

10 Review the task summary and click **Save**.

11 Run the server task immediately to instantly review the comparison results.

Reviewing the comparison results

Use this task to review the results of inventory comparison (image deviation).

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Application Control** | **Image Deviation**.
2. Locate the comparison of the gold host and endpoint.
   To quickly find the corresponding row, enter the endpoint name in the **Search Target System** field and click **Search**.
3. Click **Show Deviations**.
4. Review the comparison details.
   - Select the view type. You can organize the results based on applications or binary files.
   - Use the available filters to sort the results. Using the filters, you can view new (added), modified, and removed (missing) files. Use the **Execution Allowed Mismatch** filter to view files with changes to the execution status. Use the path filter to sort the results based on the file path.

Using dashboards and queries

Use dashboards to view the status of the endpoints and queries to review reports based on the data stored in the McAfee ePO database.

Contents

Using dashboards

Dashboards are collections of monitors that help you keep an eye on your environment. Application Control provides these default dashboards:

- **Solidcore: Inventory** dashboard allows you to observe the inventory for the endpoints
- **Solidcore: Application Control** dashboard helps you keep a check on the protected endpoints

You can create, modify, duplicate, and export dashboards. For more information on working with dashboards, see the *McAfee ePolicy Orchestrator Software Product Guide*.

Viewing queries

Use the available queries to review information for the endpoints based on the data stored in the McAfee ePO database. The following Application Control queries are available from the McAfee ePO console.

Table 6: Application Control Queries

Query	Description
Solidcore: Alerts	Displays all alerts generated in the last 3 months.
Solidcore: Application Control Agent Status	Displays the status of all endpoints with the Application Control license which are managed by the McAfee ePO console. The pie chart categorizes the information based on the client status. Click a segment to review endpoint information.
Solidcore: Attempted Violations Detected in the Last 24 Hours	Displays the attempted violation events detected during the last 24 hours. The line chart plots data on a per hour basis. Click a value on the chart to review event details.
Solidcore: Attempted Violations Detected in the Last 7 Days	Displays the attempted violation events detected during the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review event details.

Query	Description
Solidcore: Non Compliant Solidcore Agents	Lists the endpoints that are currently not compliant. The list is sorted based on the reason for non-compliance. An endpoint can be non compliant if it: • Is in Disabled, Observe, or Update mode • Is operating in limited feature activation mode • If the local command line interface (CLI) access is recovered
Solidcore: Solidcore Agent Status Report	Displays the status of all endpoints managed by the McAfee ePO console. This report combines information for both the Application Control and Change Control licenses. The pie chart categorizes the information based on the client status. Click a segment to review detailed information.
Solidcore: Solidcore Agent License Report	Indicates the number of Solidcore Agents that are managed by the by the McAfee ePO console. The information is categorized based on the license information and further sorted based on the operating system on the endpoint.
Solidcore: Policy Assignments By System	Lists the number of policies applied on the managed endpoints. Click a system to review information on the applied policies.
Solidcore: Summary Server Reboot Log - Rolling 30 Days	Displays the reboot log grouped by system name.
Solidcore: Top 10 Systems with Most Violations Detected in the Last 24 Hours	Displays the top 10 systems with the maximum number of violations in the last 24 hours. The chart includes a bar for each system and indicates the number of violations for each system. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Systems with Most Violations Detected in the Last 7 Days	Displays the top 10 systems with the maximum number of violations in the last 7 days. The chart includes a bar for each system and indicates the number of violations for each system. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Users with Most Violations Detected in the Last 24 Hours	Displays the top 10 users with the most policy violation attempts in the last 24 hours. The chart includes a bar for each user and indicates the number of policy violation attempts for each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.
Solidcore: Top 10 Users with Most Violations Detected in the Last 7 Days	Displays the top 10 users with the most policy violation attempts in the last 7 days. The chart includes a bar for each user and indicates the number of policy violation attempts for each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.

Use this task to view a query.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Reporting.**
2. Perform one of these tasks.
   - From the McAfee ePO 4.6 console, select **Queries & Reports**.
   - From the McAfee ePO 4.5 console, select **Queries**.
3. Select the **Application Control** group under **Shared Groups**.
4. Review the queries in the list.
5. Navigate to the required query and click **Run**.
   The results for the selected query are displayed.
6. Click **Close** to return to the previous page.

Maintaining your systems

After Change Control or Application Control is deployed, you can perform various tasks to maintain the endpoints. Review these topics for details about maintenance tasks.

Contents

Making emergency changes

To implement an emergency change, you can create a change window that overrides all protection and tamper proofing that is in effect. Note that memory protection (for Application Control only) remains enabled even in Update mode. You should use a change window only when the other available mechanisms cannot be used.

Complete these steps to make emergency changes.

1. Place the endpoints in Update mode.
2. Complete the required emergency changes.
3. Place the endpoints in Enabled mode.

Contents

Placing the endpoints in Update mode

Use this task to place the endpoints in Update mode to make emergency changes.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Systems** | **System Tree**.
2. Complete these steps for the McAfee ePO 4.6 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Client Task Assignment**.
The **Client Task Assignment Builder** page appears.

c Select the **Solidcore 6.0.0** product, **SC: Begin Update Mode** task type, and click **Create New Task**.
The **Client Task Catalog** page appears.

d Specify the task name and add any descriptive information.

3 Complete these steps for the McAfee ePO 4.5 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Task**.
The **Client Task Builder** page appears.

c Specify the task name and add any descriptive information.

d Select **SC: Begin Update Mode (Solidcore 6.0.0)** and click **Next**.
The **Configuration** page appears.

4 Enter the Workflow ID and any comments.
The workflow ID provides a meaningful description for the update window.

5 Click **Save** (McAfee ePO 4.6 only).

6 Click **Next**.
The **Schedule** page appears.

7 Specify scheduling details and click **Next**.

8 Review and verify the task details and click **Save**.

9 Optionally, wake up the agent to send your client task to the endpoint immediately.

Placing the endpoints in Enabled mode

Use this task to place the endpoints back in Enabled mode after you complete the required changes in the Update mode.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps for the McAfee ePO 4.6 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.

- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Client Task Assignment**.
The **Client Task Assignment Builder** page appears.

c Select the **Solidcore 6.0.0** product, **SC: End Update Mode** task type, and click **Create New Task**.
The **Client Task Catalog** page appears.

d Specify the task name and add any information.

3 Complete these steps for the McAfee ePO 4.5 console.

a Perform one of these actions.

- To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
- To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

b Click **Actions** | **New Task**.
The **Client Task Builder** page appears.

c Specify the task name and add any descriptive information.

d Select **SC: End Update Mode (Solidcore 6.0.0)** and click **Next**.
The **Configuration** page states that no other configuration settings are required for the task.

4 Click **Save** (McAfee ePO 4.6 only).

5 Click **Next**.
The **Schedule** page appears.

6 Specify scheduling details and click **Next**.

7 Review and verify the task details and click **Save**.

8 Optionally, wake up the agent to send your client task to the endpoint immediately.

Changing the CLI password

Use this task to change the default CLI password.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Policy** | **Policy Catalog**.

2 Select the **Solidcore 6.0.0: General** product.

3 Click **Duplicate** for the **McAfee Default** policy in the **Configuration (Client)** category.
The **Duplicate Existing Policy** dialog box appears.

4 Specify the policy name and click **OK**.
The policy is created and listed on the **Policy Catalog** page.

5 Open the policy.

- If you are using McAfee ePO 4.6, click the new policy.
- If you are using McAfee ePO 4.5, click **Edit Settings** for the policy.

6 Type the new password in the **CLI Settings** tab.

7 Confirm the password.

8 Click **Save**.

9 Apply the policy to the endpoints.

Collecting debug information

Prior to contacting McAfee Support to help you with a Solidcore client issue, collect configuration and debug information for your setup. This will help McAfee Support quickly identify and resolve the encountered issue. Run the Collect Debug Info client task to create an archive with endpoint configuration information and Solidcore client log files. The zip file is generated on the endpoint and its location is listed (click the record associated with the client task) on the Client Task Log page. Send the zip file to McAfee Support along with details of the encountered issue.

Use this task to create a zip file with configuration and debug information.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps for the McAfee ePO 4.6 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment** Builder page appears.

   c Select the **Solidcore 6.0.0** product, **SC: Collect Debug Info** task type, and click **Create New Task**.
   The **Client Task Catalog** page appears.

   d Specify the task name and add any descriptive information.

3 Complete these steps for the McAfee ePO 4.5 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c Specify the task name and add any descriptive information.

   d Select **SC: Collect Debug Info (Solidcore 6.0.0)** and click **Next**.
   The **Configuration** page appears.

4 Click **Save** (McAfee ePO 4.6 only).

5 Click **Next**.
The **Schedule** page appears.

6 Specify scheduling details and click **Next**.

7 Review and verify the task details and click **Save**.

8 Optionally, wake up the agent to send your client task to the endpoint immediately.

Placing the endpoints in Disabled mode

Use this task to place the endpoints in Disabled mode.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps for the McAfee ePO 4.6 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.

   c Select the **Solidcore 6.0.0** product, **SC: Disable** task type, and click **Create New Task**.
   The **Client Task Catalog** page appears.

   d Specify the task name and add any descriptive information.

3 Complete these steps for the McAfee ePO 4.5 console.

   a Perform one of these actions.

   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c Specify the task name and add any descriptive information.

   d Select **SC: Disable (Solidcore 6.0.0)** and click **Next**.
   The **Configuration** page appears.

4 Select **Force Reboot with the Task** to restart the endpoint immediately after running the task.

5 Click **Save** (McAfee ePO 4.6 only).

6 Click **Next**.
The **Schedule** page appears.

7 Specify scheduling details and click **Next**.

8 Review and verify the task details and click **Save**.

9 Optionally, wake up the agent to send your client task to the endpoint immediately.

Sending GTI feedback

Application Control includes these seeded server tasks that allow you to send feedback to McAfee on how you are currently using the GTI features.

- Solidcore: Send Event Feedback to Application Control GTI Cloud Server (disabled by default)
- Solidcore: Send Policy and Inventory Feedback to Application Control GTI Cloud Server (enabled by default to run daily)

NOTE: **No** information about individual computers or users is sent to McAfee. In addition, McAfee stores no data that can be used to track the feedback information to a specific customer or organization.

You can configure the server tasks to send information on how you are currently using one or all of these parameters.

Policies	Send information on Change Control, Application Control, and General policies. This information helps McAfee understand how you are currently using polices and applying rules and will eventually help McAfee improve the default policies and rules.
Events	Send information, such as binary name and SHA1 value for the Execution Denied, Process Hijacked, and Nx Violation Detected events. You can also choose to send information on the number of endpoints on which the event occurred with the full path of the binary file. This information helps McAfee determine how frequently and effectively Application Control blocks actions and will eventually help us improve product functionality and efficacy.
Inventory	Send detailed information for binary files, including base name, embedded application name, embedded application version, embedded version, and so on. You can also choose to send information on the number of endpoints on which the binary file is present, its execution status, and full path of the binary. Note that the feedback does not include any information to identify the endpoints, such as system name or IP address. This information helps McAfee determine how you are using (and altering) the trust score and trust level values assigned to binary files. This information will eventually help McAfee improve the GTI file reputation service.
ePO identifier	Send information on the unique McAfee ePO identifier.

Use this task to edit the server tasks.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Automation** | **Server Tasks**.
2. Select **Edit** for a server task.
   The Server Task Builder wizard opens.
3. Optionally, change the schedule status for the server task.
4. Click **Save**.

Purging data

Use this task to purge Solidcore reporting data by age or based on other parameters. When you purge data, the records are permanently deleted.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Automation** | **Server Tasks**.

2 Click **New Task**.
The **Server Task Builder** wizard opens.

3 Type the task name and click **Next**.

4 Select **Solidcore: Purge** from the **Actions** list.

5 Configure these options as required.

- **Choose Feature** - Select the reporting feature for which to purge records.
- **Purge records older than** - Select this option to purge the entries older than the specified age. This option is not applicable for features that do not have ageing criteria, such as inventory records.
- **Purge by query** - Select this option to purge the records for the selected feature that meet the query criteria. This option is only available for reporting features that support queries in McAfee ePO. Also, this option is supported only for tabular query results.

  NOTE: No seeded queries are available for purging. Prior to purging records, you must create the query from the **Menu** | **Reporting** | **Queries & Reports** (in McAfee ePO 4.6 console) or **Menu** | **Reporting** | **Queries** (in McAfee ePO 4.5 console) page.

6 Click **Next**.
The **Schedule** page appears.

7 Specify schedule details and click **Next**.
The **Summary** page appears.

8 Review and verify the details and click **Save**.

Working with Solidcore client version 5.1.5 or earlier

If you are using Application Control with Solidcore client version 5.1.5 or earlier, you can choose not to create the whitelist when you enable the software. If you defer creating the whitelist, you create it by running the SC: Initial Scan to create whitelist task.

To get suggestions on the updaters and memory-protection bypass rules to add for your setup, run the SC: Get Diagnostics for programs task.

Contents

Creating the whitelist

Use this task to create the initial whitelist (if you did not create the whitelist when enabling Application Control).

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Systems** | **System Tree**.

2 Complete these steps for the McAfee ePO 4.6 console.

   a Perform one of these actions.

      - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
      - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.

   c Select the **Solidcore 6.0.0** product, **SC: Initial Scan to create whitelist** task type, and click **Create New Task**.
   The **Client Task Catalog** page appears.

   d Specify the task name and add any descriptive information.

3 Complete these steps for the McAfee ePO 4.5 console.

   a Perform one of these actions.

      - To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
      - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c Specify the task name and add any descriptive information.

   d Select **SC: Initial Scan to create whitelist (Solidcore 6.0.0)** and click **Next**.
   The **Configuration** page appears.

4 Click **Save** (McAfee ePO 4.6 only).

5 Click **Next**.
   The **Schedule** page appears.

6 Specify scheduling details and click **Next**.

7 Review and verify the task details and click **Save**.

8 Optionally, wake up the agent to send your client task to the endpoint immediately.

Running diagnostics

When running in Enabled mode, the Solidcore protection may prevent a legitimate application from executing (if the required rules are not defined). For example, certain applications do not function correctly immediately after Solidcore is enabled. Solidcore tracks all such failed attempts made by authorized executable files to modify protected files or run other executable files. You can review information for failed attempts to identify updater rules to allow legitimate applications to run successfully. This feature is available only on the Windows platform for Solidcore client version 5.1.5 or earlier.

Use this task to retrieve a list of potential updaters and memory-protection bypass rules that can be added to a policy and applied to the endpoints. This feature helps you identify updater rules (in case certain applications do not function correctly) after the product is enabled.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Systems** | **System Tree**.
2. Complete these steps for the McAfee ePO 4.6 console.
   a. Perform one of these actions.
      - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
      - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b. Click **Actions** | **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.

   c. Select the **Solidcore 6.0.0** product, **SC: Get Diagnostics for programs** task type, and click **Create New Task**.
   The **Client Task Catalog** page appears.

   d. Specify the task name and add any descriptive information.
3. Complete these steps for the McAfee ePO 4.5 console.
   a. Perform one of these actions.
      - To apply the client task to a group, select a group in the **System Tree** and switch to the **Client Tasks** tab.
      - To apply the client task to an endpoint, select the endpoint on the **Systems** page and click **Actions** | **Agent** | **Modify Tasks on a Single System**.

   b. Click **Actions** | **New Task**.
   The **Client Task Builder** page appears.

   c. Specify the task name and add any descriptive information.

   d. Select **SC: Get Diagnostics for programs (Solidcore 6.0.0)** and click **Next**.
   The **Configuration** page appears.
4. Click **Save** (McAfee ePO 4.6 only).
5. Click **Next**.
   The **Schedule** page appears.
6. Specify scheduling details and click **Next**.
7. Review and verify the task details and click **Save**.
8. Optionally, wake up the agent to send your client task to the endpoint immediately.
9. Verify that the task was run successful by reviewing the **Menu** | **Automation** | **Solidcore Client Task Log** page. This client task collects diagnostic data from the endpoints and sends it to the McAfee ePO console.
10. Use the diagnostic recommendations to define updaters in a policy.
    a. Edit the required policy.

    b. Click **Diagnostic Suggestions** on the Updaters tab. The **Add Updater** dialog box appears.

    c. Review the listed suggestions.

    d. Select the required files to add and click **OK**.
    Exercise caution while selecting the files to mark as updaters.

    e. Save the policy.

Fine-tuning your configuration

Perform advanced configuration tasks to fine tune your configuration.

Contents

Configuring a syslog server

You can access additional servers by registering them with your McAfee ePO server. Registered servers allow you to integrate your software with other external servers. Use this task to add the syslog server as a registered server and send information (responses or Solidcore events) to the syslog server.

Task

For option definitions, click **?** in the interface.

1 Add the syslog server as a registered server.

a Select **Menu** | **Configuration** | **Registered Servers** and click **New Server**.
The **Registered Server Builder** wizard opens.

b Select **Solidcore Syslog Server** from the **Server type** list.

c Specify the server name, add any notes, and click **Next**.

d Optionally, modify the syslog server port (McAfee ePO 4.6 only).

NOTE: If you are using McAfee ePO 4.5, the default port (514) is used. You cannot alter the port when using McAfee ePO 4.5.

e Enter the server address.
You can choose to specify the DNS name, IPV4 address, or IPv6 address.

f Select the type of logs the server is configured to receive by selecting a value from the **Syslog Facility** list.

g Click **Test Syslog send** to verify the connection to the server.

h Click **Save**.

You can choose to send specific responses to the syslog server (complete step 2) or use the seeded response to send all Solidcore events to the syslog server (complete step 3).

2 Send responses to the syslog server.

a Select **Menu** | **Automation** | **Automatic Responses**.

b Click **Actions** | **New Response**.

c Enter the alert name.

d Select the **ePO Notification Events** group and **Threat** event type.

e Select **Enabled** and click **Next**.
The **Filter** page appears.

f Define the relevant filters and click **Next**.
The **Aggregation** page appears.

g Specify aggregation details and click **Next**.
The **Actions** page appears.

h Select the **Send Event To Solidcore Syslog** action.

i Specify the severity and message.
You can use the listed variables to create the message string.

j Select the appropriate syslog servers (one or more) and click **Next**.

k Review the response details and click **Save**.

3 Send all Solidcore events to the syslog server.
Application Control and Change Control include a seeded response that you can configure to automatically send all Solidcore events to the syslog server.

a Select **Menu** | **Automation** | **Automatic Responses**.

b Edit the **Send Solidcore events to Syslog Server** response to configure these options.

- Set the status to **Enabled**.
- Verify that the appropriate syslog server is selected.
- Review the message string.

  The message string is based on the Common Exchange format. Contact McAfee Support for assistance in understanding the message string.

c Save the response.

Managing the Solidcore permission sets

A permission set is a collection of permissions that can be granted to any user by assigning it to the user's account. Permission sets control the level of access users have to the different features available in the software. While user accounts provide a means for users to access and use the software, each user account is associated with one or more permission sets that define what the user is allowed to do with the software.

Permission sets only grant rights and access — no permission set removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the account grants all permissions to server tasks, that user account has all permissions for server tasks. Consider this as you plan your strategy for granting permissions to the users in your environment.

Solidcore default permission sets

When a new product extension is installed, it adds the product-specific permission sets to McAfee ePO. The Solidcore extension for Change Control and Application Control adds these permission sets:

Solidcore Admin	Provides view and change permissions across McAfee ePO features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.
Solidcore Reviewer	Provides view permissions across McAfee ePO features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.

If you need to create additional permission sets, use the Solidcore Admin permission set as a starting point and edit it as per your requirements. You can create, delete, modify, import, and export permission sets. For more information on working with permission sets, see the *McAfee ePolicy Orchestrator Software Product Guide*.

Customizing end-user notifications

If Application Control protection prevents an action on an endpoint, you can choose to display a customized notification message for the event on the endpoint. You can configure the notification to be displayed on the endpoints for these events:

- Execution Denied
- File Write Denied
- File Read Denied
- Process Hijack Attempted
- Nx Violation Detected
- ActiveX Installation Prevented
- Package Modification Prevented

Use this task to configure end-user notifications.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. Select the **Solidcore 6.0.0: General** product.
   The **McAfee Default** policy includes customizable configuration settings.
3. Click **Duplicate** for the **McAfee Default** policy in the **Configuration (Client)** category.
   The **Duplicate Existing Policy** dialog box appears.
4. Specify the policy name and click **OK**.
   The policy is created and listed on the **Policy Catalog** page.
5. Open the policy.
   - If you are using McAfee ePO 4.6, click the new policy.
   - If you are using McAfee ePO 4.5, click **Edit Settings** for the policy.
6. Switch to the **Events Custom Message** tab.
7. Select the **Show the messages dialog box when a event is detected and display the specified text in the message** option to display a message box at the endpoint each time any of the afore-mentioned events is generated.
8. Enter the helpdesk information.

Mail To	Represents the email address to which all approval requests (from endpoints) are sent.

Mail Subject	Represents the subject of email message sent for approval requests (from endpoints).
Link to Website	Indicates the website listed in the Application and Change Control Events window on the endpoints.
ePO IP Address and Port	Specifies the McAfee ePO server address and port.

9 Customize the notifications for the various types of events.

a Enter the notification message.
You can use the listed variables to create the message string.

b Select **Show Event in Dialog** to ensure that all events of the selected event type (such as Execution Denied) are listed in the **Application and Change Control Events** window on the endpoints.

10 Save the policy and apply to the relevant endpoints.

11 From the endpoints, users can review the notifications for the events and request for approval for certain actions.

a Right-click the McAfee Agent icon in the system tray on the endpoint.

b Select **Quick Settings** | **Application and Change Control Events**.
The **Application and Change Control Events** window appears.

c Review the events.

d Request approval for a certain action by selecting the event and clicking **Request Approval**.

FAQs

What is an Alternate Data Stream (ADS)? Does Change Control monitor changes to ADSs?

On the Microsoft NTFS file system, a file consists of multiple data streams. One stream holds the file contents and another contains security information. You can create alternate data streams (ADS) for a file to associate information or other files with the existing file. In effect, alternate data streams allow you to embed information or files in existing files. The ADSs associated with a file do not affect its contents or attributes and are not visible in Windows Explorer. So, for practical purposes, the ADSs associated with a file are hidden. Malicious users can misuse the ADS feature to associate malicious files with other files without the malicious files being detected.

Change Control monitors changes to Alternate Data Streams (ADS) associated with files on the Windows platforms. For a monitored file, all ADS-related changes, including stream creation, modification, updation, deletion, and attribute changes are reported as events. If you are also using Application Control, any executable programs (associated as an ADS with an existing file) are prevented from running. To disable ADS monitoring execute the SC: Run Commands client task to run the **sadmin features disable mon-ads** command on the endpoint.

Why am I not receiving the events for user account activity for an endpoint?

User account activity is tracked by default (no configuration is needed) for all endpoints on which Change Control is deployed and enabled. However, you must ensure that the Audit Policy is configured on the Windows operating system to allow generation of user activity events.

To successfully track user account activity for an endpoint, verify the Audit Policy configuration for the endpoint.

1. Navigate to **Control Panel** | **Administrative Tools**.
2. Double click **Local Security Policy**.
3. Select **Local Policies** | **Audit Policy**.
4. Double click the **Audit account logon events** policy.
5. Select **Success** and **Failure** and click **OK**.
6. Repeat steps 4 and 5 for the **Audit account management** and **Audit logon events** policies.

What are the implications of recovering the local CLI access for an endpoint?

To troubleshoot or debug issues, you might need to recover the local CLI access for an endpoint. Note that recovering the local CLI for an endpoint prevents the enforcement of policies from McAfee ePO to the endpoint. This implies that when the CLI is recovered for an endpoint, no existing or new policies (created on the McAfee ePO console) are applied to that endpoint.

What is the significance of label specified in a policy while configuring updaters, installers, and trusted users?

The specified labels help you correlate the generated events with the actions performed by the trusted resources. For example, when an event is generated for an action performed by a trusted user, the **Workflow ID** attribute for the event includes the label specified for the trusted user.

How do I unsolidify a file, folder, or volume?

To unsolidify a file, folder, or volume, run the **SC: Run Commands** client task with the sadmin unso <resource name> command.

Do Change Control and Application Control work in Network Address Translation (NAT) environments?

If the McAfee ePO server is able to communicate with the McAfee Agent in a NAT environment, Change Control and Application Control will work.

How can I trust custom scripts and applications developed for use within my organization?

Sign the scripts and applications with a self-generated certificate, then trust the certificate.

1. Perform one of these actions.
   - Locate your certificate if you have an existing certificate.
   - Generate a X.509 certificate pair using a tool, such as **makecert.exe** (see http://msdn.microsoft.com/en-us/library/bfsktky3%28VS.80%29.aspx).
2. Export the certificate in PEM (Base-64 encoded X.509 - .CER) format.
3. Upload the certificate and add it to an Application Control policy as a trusted publisher.
4. Apply the policy to the endpoints.
5. Use the certificate to sign and verify all custom scripts and in-house applications. This can be done using a tool, such as **SignTool.exe**.

   NOTE: When working with scripts, convert the script into a self extracting executable file, then sign the file.
6. Define the internal certificate as a trusted publisher.

Can I script sadmin commands?

Yes, you can script sadmin commands. Note that while recovering the CLI, you are prompted to enter to password. To achieve this within a script, suffix the sadmin recover command with -z <password>.

Run Commands client task

Use this page to run CLI commands remotely on the endpoints.

Option definitions

Option	Definition
Run Command	Type the CLI command you want run on the endpoints.
Requires Response	Select this option if you want receive the result of the command. The command output is available on the **Automation** | **Solidcore Client Task Log** page on the McAfee ePO console.

Pull Inventory client task

Use this page to fetch the software inventory for one or more endpoints.

NOTE: No additional configuration is required to run this client task.

After this task runs successfully, you can review the inventory details for the endpoints and define new rules. Use the **Application Control** | **Inventory** | **Inventory by Applications** and **Application Control** | **Inventory** | **Inventory by Systems** pages to define rules.

Initial Scan to create whitelist client task

Application Control requires the creation of a list of all trusted executable files present on the endpoint system (known as the whitelist). The one-time activity of creating the whitelist is known as whitelisting or solidification.

If you are using Application Control with Solidcore client version 5.1.5 or earlier, you can choose not to create the whitelist when you enable the software. If you have deferred creating the whitelist, you can create it by running the **Initial Scan to create whitelist** client task.

NOTE:

- This client task is required only if you deselected the **Perform Initial Scan to create whitelist** option when running the **Enable** client task.
- No additional configuration is required to run this client task.

End Update Mode client task

Run this task to close the update mode window on the required endpoints.

NOTE: No additional configuration is required to run this client task.

Get Diagnostics for programs client task

If you are using Solidcore client version 5.1.5 or earlier, run the SC: Get Diagnostics for programs client task to get suggestions on the updaters and memory-protection bypass rules to add for your setup. This task retrieves a list of potential updaters that can be added to an Application Control policy and applied on the endpoints.

NOTE: No additional configuration is required to run this client task.

Enable client task

Use this page to enable Solidcore client on the endpoints.

Option definitions

Option	Definition
Solidcore Client	• **Platform** — Use this option to select the platform on which to enable the software. • **Sub Platform** — Use this option to select the operating system on which to enable the software. • **Version** — Select this Solidcore client version to enable on the endpoints.

Enable	• **Change Control** — Use this option to enable the Solidcore client to track changes.
	• **Application Control** — Use this option to enable the Application Control license on the endpoints. Selecting this will build an inventory of all binary and executable files on the endpoint.
	  • **Initial Scan Priority** — Select an option to specify the priority of the thread that is run to create the whitelist on the endpoints.
	  • **Perform Initial Scan to create whitelist** (only available for 5.1.5 or earlier) — Use this option to create the whitelist when enabling Application Control.

Activation Options	• **Limited Feature Activation** — Use this option to enable limited Application Control features without restarting the endpoints. The endpoints are not restarted and limited features of Application Control (memory protection features are unavailable) are activated. Memory protection features are available only after the endpoint is restarted. • **Full Feature Activation** — Use this option to enable all Application Control features (requires you to restart the endpoints). The endpoints are restarted, whitelist created, and all features of Application Control including Memory Protection are active. Restarting the endpoints is necessary to enable the memory protection features. The endpoint is restarted 5 minutes after the client task is received at the endpoint. A popup message is displayed on the endpoint before the endpoint is restarted.
Observe Mode	**Start Observe Mode** — Use this option to place the endpoints in Observe mode.
Inventory	**Pull Inventory** — Use this option to fetch the inventory (including the created whitelist) for the endpoints. After it is fetched, it is available on the McAfee ePO console. We recommend that you select this option because inventory information is used in multiple workflows available from McAfee ePO.
Reboot (only available for 5.1.5 or earlier)	**Force Reboot with the Task** — Use this option to restart the endpoint immediately after running the task. NOTE: A restart of the endpoint is necessary to bring the changes into effect.

Disable client task

Use this page to disable Solidcore client on the endpoints.

Option definitions

Option	Definition
Force Reboot with the task	Use this option to restart the endpoint immediately after running the task. NOTE: A restart of the endpoint is necessary to bring the changes into effect.

Change Local CLI Access client task

Use this page to allow or restrict access to the CLI console access on the endpoints.

Option definitions

Option	Definition
Change CLI Status	• **Allow** — Use this option to allow users on the endpoints to access McAfee Solidcore Client CLI console without any authentication. NOTE: During this CLI console state, any changes in configuration, policies, tasks pushed from ePO console will not be enforced on the endpoint. The CLI Status needs to be **Restrict** or **Lockdown** to enforce any changes to endpoint. • **Restrict** — Use this option to allow only authorized users to access McAfee Solidcore Client CLI console on the endpoints. To access the CLI console, users need to provide the password set in the **McAfee Default** policy in the **Configuration (Client)** category.

Collect Debug Info client task

Prior to contacting McAfee Support to help you with a Solidcore client issue, collect configuration and debug information for an endpoint. This client task will scan the endpoint and create an archive with system information and Solidcore client log files that can be used for debugging.

The zip file is generated on the endpoint and its location is listed (click the record associated with the client task) on the **Automation** | **Solidcore Client Task Log** page.

NOTE: No additional configuration is required to run this client task.

Begin Update Mode client task

To authorize approved changes to endpoints, you can open a change window during which users or programs can make changes. Use this page to allow authorized or approved changes to the endpoints.

Option definitions

Option	Definition
Workflow ID	Type a meaningful label or ID for the update mode window. Any changes made during the update mode will be tagged with the specified label or ID.
Comments	Type a description for the update mode window.

Observe Mode client task

Use this page to place the Solidcore client on the endpoints in Observe mode.

Option definitions

Option	Definition

Observe Mode	Allows you to specify whether to begin or end Observe mode.
	• **Start Observe Mode** — Use this option to place the endpoints in Observe mode.
	  • **Workflow ID** — Specifies the workflow ID that can be used to track the Observations generated in Observe mode.
	  • **Comments** — Allows you to provide any comments or additional information, if needed.
	• **End Observe Mode** — Use this option to remove the endpoints from Observe mode.
	  • **Enable Solidcore client** — Use this option to place the endpoints in Enabled mode.
	  • **Disable Solidcore client** — Use this option to place the endpoints in Disabled mode.

Whitelist Options	Allows you to indicate whether to update the whitelist for the endpoints based on the changes made in Observe mode. Select the **Update changes made in Observe Mode to Whitelist** option to update the whitelist. If you have modified existing files on the endpoint running in Observe mode, make sure you update the whitelist based on changes made to the endpoint. If you do not select this option, all changes made on the endpoints during Observe mode are discarded.

Advanced tab

Use this page to define advanced exclusion filters to exclude changes by using a combination of conditions. You can designate a set of files, processes or programs, events, registry keys, and users to exclude from being monitored for changes.

Use this page to define rules to prune routine system-generated events not relevant for monitoring or auditing.

Option definitions

Option	Definition
Add Rule	Adds new advanced filtering rule. Configure these options as required. • **File** — Use this option to specify the comparison operator and the file name or directory to be excluded from being monitored. • **Event** — Use this option to specify the comparison operator and the Solidcore event to be excluded from being monitored. • **Program** — Use this option to specify the comparison operator and the process or program to be excluded from being monitored. • **Registry** — Use this option to specify the comparison operator and the registry key to be excluded from being monitored. This option is available only for the Windows platform. • **User** — Use this option to specify the comparison operator and the user name to be excluded from being monitored.
Delete	Deletes the selected advanced filter rule.

Users tab

By default, changes made to endpoints by all users are monitored. You can create a **Integrity Monitoring Rules** policy to exclude a set of users from being monitored.

Use this page to exclude users from being monitored.

Option definitions

Option	Definition
Add	Opens the **Add User** dialog box. • **User** — Type the name of the user to exclude from being monitored. NOTE: For a domain user, specify the user name in **domain\user** format. • **Exclude** — Excludes specific users from being monitored. • **OK** — Click this option to save the specified rules. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add User** dialog box with information for a selected rule. Edit the user name as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Program tab

You can choose to track or not track all file or registry changes made by a program. When a monitored process or program makes a change, an event is generated on the endpoint and sent to the McAfee ePO server.

Use this page to add processes or programs to be included or excluded from being monitored for changes.

Option definitions

Option	Definition
Add	Opens the **Add Program** dialog box. • **Program** — Specify the process or program to be monitored for changes. • **Include** — Use this option to monitor changes made by the specified process or program. • **Exclude** — Use this option to exclude any specific process or program from being monitored. • **OK** — Click this option to monitor changes done by the specified process or program. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add Program** dialog box with information for a selected rule. Edit the process or program as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Extension tab

You can monitor specific file types by specifying the file extensions to be included for or excluded from monitoring. When a file of a monitored file type is modified, an event is generated on the endpoint and sent to the McAfee ePO server.

Use this page to add file extension to be included or excluded from being monitored for changes.

Option definitions

Option	Definition
Add	Opens the **Add Extension** dialog box. • **Extension** — Type the file extension to be monitored for changes. • **Include** — Use this option to monitor changes to the specified file extension. • **Exclude** — Use this option to exclude a specific file extension from being monitored. • **OK** — Click this option to monitor changes to the specified file extension. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add Extension** dialog box with information for a selected rule. Edit the file extension as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Registry tab

On the Windows platform, you can define rules to monitor registry keys. You can choose to include or exclude the registry key for monitoring. When a monitored registry key is modified, an event is generated on the endpoint and sent to the ePO server.

Use this page to add registry keys to be included or excluded from being monitored for changes.

Option definitions

Option	Definition
Add	Opens the **Add Registry** dialog box. • **Registry** — Type the registry key to be monitored for changes. • **Include** — Use this option to monitor changes to the specified registry key. • **Exclude** — Use this option to exclude the registry key from being monitored. • **OK** — Click this option to monitor changes to the specified registry key. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add Registry** dialog box with information for a selected rule. Edit the registry key as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

File tab

You can designate a set of files to be included or excluded from being monitored for changes. When a monitored file is changed, an event is generated on the endpoint and sent to the ePO server.

Use this page to add files or directories to be included or excluded from being monitored for changes.

Option definitions

Option	Definition
Add	Opens the **Add File** dialog box. • **File** — Type the name of the file or directory to be monitored for changes. • **Include** — Use this option to monitor changes to the specified file or directory. • **Exclude** — Use this option to exclude a specific file or directory from being monitored. • **Enable content change tracking** — Use this option to track content and attribute changes for the file. • **File encoding** — Select an option to specify the encoding for the file for which you are tracking content changes. • **OK** — Click this option to monitor changes to the specified file or directory. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add File** dialog box with information for a selected rule. Edit the file name or directory as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Read Protect tab

Define read-protection rule to prevent users from reading the content of specified files, directories, and volumes.

NOTE: By default, the read protection feature is disabled at the endpoints. To enable the read protection feature, create a **Run Commands** client task with the features enable deny-read command.

Use this page to read-protect critical files or directories.

Option definitions

Option	Definition
Add	Opens the **Add File** dialog box. • **File** — Type the name of the file to protect. • **Include** — Use this option to read-protect the specified file or directory. • **Exclude** — Use this option to exclude the specified file or sub directory from read protection. • **OK** — Click this option to read-protect the specified file or directory. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add File** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Write Protect File tab

Applying write-protection rules renders specified files as read-only thereby protecting your valuable data from unauthorized updates.

Use this page to prevent unauthorized changes to the critical files.

Option definitions

Option	Definition
Add	Opens the **Add File** dialog box. • **File** — Type the name of the file or directory to protect. • **Include** — Use this option to write-protect the specified file. • **Exclude** — Use this option to exclude the file from write protection. • **OK** — Click this option to write-protect the specified file. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add File** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Write Protect Registry tab

Applying write-protection rules to registry keys renders the specified keys as read-only thereby protecting critical keys from unauthorized updates.

Use this page to prevent unauthorized changes to the critical registry keys.

Option definitions

Option	Definition
Add	Opens the **Add Registry** dialog box. • **Registry** — Type the registry key or hive to protect. • **Include** — Use this option to write-protect the specified registry key or hive. • **Exclude** — Use this option to exclude the specified registry key or hive from write protection. • **OK** — Click this option to write-protect the specified registry key or hive. • **Cancel** — Click this option to exit without saving the settings.
Edit	Opens the **Add Registry** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Deletes the selected rule from the policy.

Updaters tab

When a program is configured as an updater, it can install new software and update existing program code (including itself) installed on the endpoint. Note that updaters work at a global-level and are not application-specific. After a program is defined as an updater, it can modify any protected file.

Use this page to add updaters authorized to perform updates on the protected endpoints (without any user intervention).

Option definitions

Option	Definition

Add	Opens the **Add Updater** dialog box. Configure these options as required.
	• **Binary** — Type the location of the executable or binary file.
	• **Updater Label** — Type a identification label. All changes made by the binary are tagged with the specified label.
	• **Condition** — Select one of these options:
	  • **None** — Select this option to authorize the updater without any conditions.
	  • **Parent** — Select this option to allow the binary file to run as an updater only if it is launched by the specified parent.
	  • **Library** — Select this option to allow the binary file to run as updater only when it has loaded the specified library.
	• **Disable Inheritance** — Select this option to disable inheritance for the updater. For example, if Process A (that is set as an updater) launches Process B, disabling inheritance for Process A ensures that Process B will not become an updater.
	• **Suppress Events** — Select this option to suppress events generated for actions performed by the updater.
	• **OK** — Click this option to add and authorize the updater.
	• **Cancel** — Click this option to exit without saving the updater details.

Edit	Opens the **Edit Updater** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.
Diagnostic Suggestions (relevant only for 5.1.5 or earlier versions)	Select this option to review available diagnostic recommendations. Use the suggestions to define rules to add updaters relevant for your setup.

Trusted Users tab

Use this page to add trusted users.

Option definitions

Option	Definition
Add	Opens the **Add Trusted Users** dialog box. • **Domain\User** — Type the domain name and logon name of the user. • **User Label** — Type an identification label. All changes made by the user are tagged with the specified label. • **Name** — Type the name of the user. • **OK** — Click this option to add the user. • **Cancel** — Click this option to exit without saving the user details.
Edit	Opens the **Edit Trusted Users** dialog box with information for a selected rule. Edit the user details as required, then click **OK**.
Remove	Select this option to delete the selected rule.
AD Import	Opens the **Import from Active Directory** dialog box. • **Active Directory Server** — Select the required registered server. • **Global Catalog Search** — Select this option to search for users in the catalog (only if the selected Active Directory is a Global Catalog server). • **Search for** — Select whether to search for users or groups. • **Search By** — Select whether to search for Users by UPN (User Principal Name) or SAM account name. NOTE: Note that your search will determine the authorized user. Ensure that you use the trusted account to log on to the endpoint. If you use the UPN name while adding a user, ensure that the user logs on with the UPN name at the endpoint to enjoy trusted user privileges. • **User Name** — Type the user name search string. The Contains search criteria is applied for the specified user name. • **Group Name** — Type the group name if you want to restrict users to a group. NOTE: You cannot directly add a group present in the Active Directory to a policy. To authorize all users in a group, add the user group to a rule group and include the rule group in a policy. Using groups ensures that all changes to a user group automatically cascade across all rule groups and associated policies. • **Find** — Click this option to search for the specified user or group name.

Binary tab

Use this page to allow or ban a binary based on its name or checksum.

Option definitions

Option	Definition

Add	Opens the **Add Binary** dialog box. Create a file name rule by specifying the file name, optionally with one or more directories above the system tree or a checksum rule to authorize binary by its SHA1 checksum.
	• **Rule name** — Type the name of a program.
	• **Allow/Ban** — Specify if the program is trusted or not.
	• **Rule Type** — Select one of these options.
	  • **File** — Select this option to add the binary file name.
	  • **Checksum** — Select this option to add the checksum of the binary file.
	• **Name/SHA1** — This field will be either Name or SHA1 depending on the Rule Type.
	• **OK** — Click this option to add the binary file or checksum.
	• **Cancel** — Click this option to exit without saving the binary details.

Edit	Opens the **Edit Binary** dialog box with information for a selected rule. Edit the details as required, then click **OK**.
Remove	Deletes the selected rule.

Publishers tab

Use this page to add a certificate or publisher.

Option definitions

Option	Definition

Add	Opens the **Add Publisher** dialog box.
	• **Search By** — Select one of these categories based on how you want to search for publishers.
	  • **Issued to** — Use this option to search for publishers based on the name of the organization that publishes the certificate.
	  • **Issued by** — Use this option to search for publishers based on the name of the signing authority.
	  • **Extracted From** — Use this option to search for publishers based on the file name from which the certificate was extracted.
	  • **Friendly Name** — Use this option to search for publishers based on the user-specified name for the certificate.
	  • **Search** — Use this option to search for the specified publisher.
	• **Add Publisher(s) as Updater** — Select this option to allow the applications signed by the selected publishers to make changes to the executable files or launch any new application on the endpoints.
	• **Updater Label** — Type an identification label used to tag all the changes made by the executable file signed by the publisher.
	• **OK** — Click this option to add the publisher.
	• **Cancel** — Click this option to exit without saving the publisher details.

Edit	Opens the **Edit Publisher Details** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.

Installers tab

Use this page to add installers authorized to install and update the software on the endpoints.

Option definitions

Option	Definition

Add	Opens the **Add Installer** dialog box.
	• **Search By** — Use this option to search for the required installer.
	  • **Installer Name** — Type the name of the installer.
	  • **Vendor** — Type the name of the vendor who publishes the installer.
	  • **Search** — Use this option to search for the specified installer or vendor.
	• **Installer Label** — Type an identification label used to tag all the changes made by the installer.
	• **OK** — Click this option to add the installer.
	• **Cancel** — Click this option to exit without saving the installer details.

Edit	Opens the **Edit Installer Details** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.

Trusted Directories tab

Use this page to add a trusted directory, such as a shared network drive to allow users to install any software from the directory.

Option definitions

Option	Definition

Add	Opens the **Add Path** dialog box.
	• **Path** — Type the location of the directory that you want to add as trusted directory. Specify the UNC pathname for the directory.
	  • **Include** — Use this option to include the specified directory as a trusted directory.
	  • **Exclude** — Use this option to exclude a specific folder or subfolder within a trusted directory.
	  • **Make programs executed from this directory updaters** — Use this option to allow the applications stored on the trusted directory to make changes to the executable files or launch a new application on the endpoints.
	  • **OK** — Click this option to add the trusted directory.
	  • **Cancel** — Click this option to exit without saving the rule.

Edit	Opens the **Edit Path** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.

Exceptions tab

Use this page to define rules to override or bypass the applied memory-protection techniques.

Option definitions

Option	Definition
Add	Opens the **Add Attribute** dialog box. • **File** — Type the name of the file that you want to bypass from the applied memory-protection techniques. • **Bypassed from CASP (for Windows 32-bit)** — Use this option to bypass the selected file from the Critical Address Space Protection (CASP) technique. • **Bypassed from DEP (for Windows 64-bit)** — Use this option to bypass the selected file from the Data Execution Protection (DEP) technique. • **Bypassed from Call Context Verification (for Windows 64-bit)** — Use this option to bypass the selected file from the Call Context Verification technique. • **Bypassed from ASLR (for Windows 64-bit)** — Use this option to bypass the selected file from the Address Space Layout Randomization technique. • **Process Context File Operations Bypass** — In certain scenarios, Application Control can prevent legitimate applications from running. Use this option to define a bypass rule for a file on 32-bit and 64-bit Windows platforms. Use this option judiciously because it may impact default Application Control functionality. • **Parent** — Use this option to specify the parent to allow the file to bypass the memory-protection features if it is launched by the specified parent. This option is applicable only for the Process Context File Operations Bypass and Bypassed from ASLR options. • **OK** — Click this option to add the rule. • **Cancel** — Click this option to exit without saving the rule. NOTE: Contact McAfee Support for information on other deprecated memory-protection techniques, such as API Mangling, Decoying, and Virtual Address Space Randomization (VASR).
Edit	Opens the **Edit Attribute** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.
Diagnostic Suggestions (relevant only for 5.1.5 or earlier versions)	Select this option to review available diagnostic recommendations. Use the suggestions to define rules to add updaters relevant for your setup.

Search Image Deviation Summary page

Use this page to view image deviation results. Using the Image Deviation feature, you can compare the inventory of an endpoint with the inventory of a designated gold system. This page provides a summary of the image comparison and lists changes, such as modifications, deletions or additions to the inventory of the endpoint (as compared to the inventory of the gold system).

Option definitions

Option	Definition
Search Target System	Use this option to search for image deviation summary for a target system. Specify the name of the target system, and then click **Search**.
Options	• **Show Deviations** — Opens the **Image Deviation Details** page. • **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email the image deviation summary. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the **Binaries** pane.

Image Deviation Details page

Use this page to view the image deviation details, including deviation type, path, and checksum. You can sort the details based on applications or binary files.

Option definitions

Option	Definition
Filter	• **Filter by Deviation Type** — Select the image deviation type to use to filter the image deviation details. • **Filter by Path** — Specify the file path to use to filter the image deviation details. • **Update Filters** — Click to filter the image deviation details based on the specified type and path.
View	Allows you to sort the details either by applications or binaries. • **Applications** — Use this option to view the **Applications** pane that sorts all files based on the associated application. All listed applications and binary files are sorted into Good, Bad, and Unclassified categories. Click **App Details** to view the details for a selected application. • **Binaries** — Use this option to view a list of all the binary files.
Actions	• **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email the image deviation details. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the **Binaries** pane.
Back	Click to return to the previous page.
Close	Click to return to the Search Image Deviation Summary page.

Solidcore Client Task Log page

Use this page to view status of the Solidcore Client Tasks run on the endpoints.

Option definitions

Option	Definition
Filter	Allows you to filter the listed details based on these criteria: • **System Name** — Use this option to filter information based on the system name. • **Time** — Use this option to review information for the specified time period. • **Task Name** — Use this option to filter information based on the task name. • **Task Status** — Use this option to filter information based on whether the client task is in progress, executed successfully, or failed. • **Command Status** — Use this option to filter information based on whether the command executed through the client task was successful or not. • **Search** — Use this option to filter based on the specified criteria.
Actions	Specifies the actions that you can perform on the selected client task log, including: • **Delete** — Removes the selected record from the page.
Options	• **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email the client task log.

Inventory by Applications page

Use this page to review and manage the software inventory for one or more endpoints in your setup. You can access this page by selecting:

- **Menu** | **Application Control** | **Inventory** | **Inventory By Applications** (allows you to manage inventory for all endpoints in your setup)
- **Menu** | **Application Control** | **Inventory** | **Inventory By Systems** | **View Inventory** (allows you to manage inventory for a single endpoint)

Option definitions

Option	Definition

Views and Filters	• **Views** — View the inventory details using these options:
	  • **Application** — Use this option to filter the inventory based on the applications on the endpoints.
	  • **Binary Name** — Use this option to view all binary files filtered by name.
	  • **Binary SHA1** — Use this option to view all binary files filtered by the checksum value.
	  • **Vendor** — Use this option to filter the inventory based on the vendor name.
	  • **Trust Level (Enterprise)** — Use this option to filter the inventory based on the enterprise trust level.
	• **Filter** — Enter a search string to filter the inventory details. The search string can be used in conjunction with the available views.
	• **Search** — Click to filter the displayed results based on the specified view and filter criteria.

Saved Filters	Use these filters to view selected binary files. • **Add Saved Filter** — Opens the Select View page that allows you to define a new filter. Use the available properties to define the filter. • **None** — Use this option to clear an applied filter. • **All Bad Binaries** — Use this option to view all binary files for which **Enterprise Trust Level** is set to **Bad**. • **Allowed Bad Binaries** — Use this option to view all binary files for which **Enterprise Trust Level** is set to **Bad** and that are allowed on your enterprise. • **Allowed Unclassified Signed Binaries** — Use this option to view all binary files that are allowed on your enterprise, are signed by a publisher, and for which **Enterprise Trust Level** is set to **Unclassified**. • **Allowed Unclassified Unsigned Binaries** — Use this option to view all binary files that are allowed on your enterprise, are not signed by a publisher, and for which **Enterprise Trust Level** is set to **Unclassified**. • **Banned Good Binaries** — Use this option to view all binary files that are banned on your enterprise and for which **Enterprise Trust Level** is set to **Good**.
Applications	Use this pane to view inventory details in the Application view. In the tree, all applications and binary files are sorted into Good, Bad, and Unclassified categories. • **Collapse All** — Click to minimize all expanded nodes in the Applications pane.

Option	Definition
	• **App Details** — Opens the **Application details** page with details for the application selected in the Applications pane.
Vendors	Use this pane to view inventory details in the Vendor view. For each vendor, you can view the Good, Bad, and Unclassified categories.
Binaries	Use this pane to view binary information in the Binary Name and Binary SHA1 views. In the Application and Vendor views, this pane lists the binary files associated with the node selected in the Applications or Vendors pane. • **Hide Filter/Show Filter** — Use these to hide or show the filters in the pane. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the binary list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected in the Binaries pane.
Actions	• **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email inventory details. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the **Binaries** pane. • **Allow Binaries** — Opens the **Allow or Ban Binaries** wizard. Use this wizard to allow a binary file by adding it to the whitelist or defining a rule. • **Ban Binaries** — Opens the **Allow or Ban Binaries** wizard. Use this wizard to ban a binary file by defining a rule. • **Change Enterprise Trust Level** — Opens the **Change Enterprise Trust Level** dialog box that allows you to edit the enterprise trust level for the selected file.

Inventory by Systems page

Use this page to review and manage the inventory for selected endpoints.

Option definitions

Option	Definition
Saved Filters	Use these filters to view selected binary files. • **Add Saved Filter** — Opens the Select View page that allows you to define a new filter. Use the available properties to define the filter. • **None** — Use this option to clear an applied filter. • **System with Allowed Bad Binaries** — Use this option to view all endpoints on which binary files for which **Enterprise Trust Level** is set to **Bad** are allowed. • **Systems with Bad Files** — Use this option to view all endpoints on which binary files for which **Enterprise Trust Level** is set to **Bad** are present.
Systems	Use this pane to view information for the endpoints in your setup. • **View Inventory** — Use this option to view inventory details for the associated endpoint. • **Fetch Inventory** — Use this option to fetch inventory details for the associated endpoint. • **Hide Filter/Show Filter** — Use these to hide or show the filters in the pane. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected in the Systems pane.
Actions	• **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email inventory details. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the **Binaries** pane.

Binary Details page

Use this page to review details for a binary file. You can access this page when you click a binary name (in the **Binaries** pane) from any of these pages:

- **Inventory By Applications** page
- **Inventory Details** page (opens when you click **View Inventory** for an endpoint on the **Inventory By Systems** page)

Option definitions

Option	Definition
Cloud Trust Score	Lists the cloud trust score for the selected binary file. Click the trust score value to review the details obtained from the GTI server for the binary file.
Binary Properties	Lists properties, such as version and trust level for the selected binary file. Click **More** to view all properties for the selected binary file.
Execution Status in Enterprise Inventory	This monitor indicates the current status of the selected binary file in your enterprise.
Systems for this Binary	This pane lists all the endpoints on which the selected binary file is present. • **Hide Filter/Show Filter** — Use these to hide or show the filter options in the pane. • **Preset** — Select an option to filter the systems list based on the whether the binary file is allowed or banned on the endpoints. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected in the **Binaries** pane.
Actions	• **Ban/Allow** — Opens the **Allow or Ban Binaries** wizard that allows you to ban the binary file by defining a rule. • **View Events** — Opens the **Events** page that allows you to view events generated for the binary file. • **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email binary details. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the **Systems for this Binary** pane.

Application Details page

Use this page to review details for an application. You can access this page from these pages:

- **Inventory By Applications** page by clicking **App Details** for an application selected in the **Applications** or **Vendors** pane
- **Inventory Details** page (opens when you click **View Inventory** for an endpoint on the **Inventory By Systems** page) by clicking **App Details** for an application selected in the **Applications** or **Vendors** pane
- **Image Deviation Details** page by clicking **App Details** for an application selected in the **Applications** pane

Option definitions

Option	Definition
Application Properties	Lists properties, such as vendor and trust level for the selected application.
Systems	This pane lists all the endpoints on which the selected application is present. • **Hide Filter/Show Filter** — Use these to hide or show the filter options in the pane. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected in the **Systems** pane.
Binaries	This pane lists all the binary files associated with the selected application. • **Hide Filter/Show Filter** — Use these to hide or show the filter options in the pane. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected in the **Binaries** pane.
Actions	The following actions are available from the **Systems** and **Binaries** panes. • **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email application details. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the **Binaries** pane. The following actions are available only from the **Systems** pane. • **Fetch Inventory** — Use this option to fetch inventory details for the selected endpoint. • **Import Inventory** — Use this option to import inventory details for the selected from an XML file. The inventory for the selected endpoint is updated based on the inventory details included in the XML file. • **View Inventory** — Use this option to view inventory details for the selected endpoint.

Solidcore Alerts page

Use this page to view Solidcore-related alerts.

Option definitions

Option	Definition
Options	• **Export Table** — Opens the **Export** page. Use this to specify the format and the package of files to be exported. You can save or email the Solidcore alerts.
Actions	Specifies the actions that you can perform on the selected alerts, including: • **Dismiss** — Select this option to dismiss the selected Solidcore alert(s).
Select all in this page	Use this option to select all the Solidcore alerts displayed on the current page.
Select all in all pages	Use this option to select all the Solidcore alerts displayed on all pages.

Edit Filter Criteria page

Use this page to select specific properties with which you want to filter the Solidcore Events.

Option definitions

Option	Definition
Available Properties	Specifies the properties that can be selected and configured as criteria to filter Solidcore Events.
Property	Lists the name of the properties that you select from the list of available properties.
Comparison	Specifies the comparison operator to use for filtering the property value.
Value	Specifies the property value to filter.
Remove Filter	Removes the advanced filters and returns to the Solidcore Events page.
Update Filter	Updates the advanced filters and returns to the Solidcore Events page to display filtered information.

Solidcore Events page

Use this page to view all Solidcore events generated for the managed endpoints.

Option definitions

Option	Definition
Filter	Allows you to filter the displayed events based on specified criteria, including: • **Time Filter** — Use this option to filter events generated in the specified time period. • **System Tree Filter** — Use this option to filter events generated for the specified group or subgroup. • **Advanced Filters** — Opens the **Edit Filter Criteria** page. Use this page to select properties to filter the content displayed on the Solidcore Events page.
Options	• **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the **Solidcore Events** page.
Actions	Specifies the actions that you can perform on the selected events, including: • **Show Related Systems** — Takes you to a page where you can view and take action on the systems where selected events occurred. • **Dismiss Observations** — Use this option to ignore or dismiss one or more observations. • **Exclude Events** — Use this option to exclude or ignore events not required to meet compliance requirements. • **Reconcile Events** — Use this option to manually reconcile events by correlating the events with change tickets and marking the events as authorized or unauthorized.
Select all in this page	Use this option to select all the Solidcore events displayed in the current page.
Select all in all pages	Use this option to select all the Solidcore events displayed in all pages.

Edit Solidcore License Information page

After you install the Solidcore extension, provide the license keys to enable the corresponding product features. The license key determines the features that will be enabled. Any or all features can be enabled and used at a time.

Use this page to edit Solidcore license information for Application Control, Change Control, Integrity Control, and Reconciliation. You can also configure settings for other features, such as GTI cloud, inventory, observe mode, and reconciliation.

Option definitions

Option	Definition
License Information	• **Change Control** — Type the Change Control license key downloaded with the product from McAfee download website. • **Application Control** — Type the Application Control license key downloaded with the product from McAfee download website. • **Integrity Control** — Type the Integrity Control license key downloaded with the product from McAfee download website. • **Reconciliation** — Type the Reconciliation license key downloaded with the product from McAfee download website.
General	• **GTI Cloud: Cloud Trust Score of binary below which alert will be generated** — Specify the cloud trust level for event generation. Events are generated for all binary files for which the cloud trust level is below this value. If needed, you can set up responses to receive a notification for these events. • **GTI Cloud: Enable Fetching Cloud Trust Levels of App Control Inventory Binaries from Cloud** — Specify whether or not the software synchronizes with GTI file reputation service to fetch information for binary files. • **Inventory: Ignored Extensions in Inventory** — Specify the files (by specifying the file extension) you do not want to manage in the inventory. No information for the specified file types is stored in the inventory tables. • **Observe Mode: Generic Launcher Processes** — Specify the critical processes for your setup. Certain processes on the Windows operating system, such as explorer.exe and iexplore.exe are launcher processes that are vital to the operating system. Although observations are generated for Generic Launcher processes, no suggestions are provided. • **Reconciliation: Enable Ticket Based Enforcement** — Use this option to enable ticket-based enforcement. Using ticket-based enforcement, you can ensure seamless system updates without any manual intervention. Once integrated with a Change Management System (CMS), changes to an endpoint are permitted only when a ticket is approved in the ticketing system. • **Reconciliation: Ticket Based Enforcement Interval In Seconds** — Use this option to specify the time interval (in seconds) between consecutive requests to poll the CMS.

Scan a Software Repository server task

Use this page to schedule a scan on a network share on a regular basis to:

- Extract the certificates associated with one or more signed binary files present on the share
- Add installers present on the share

Option definitions

Option	Definition
Software Repository Path	Type the path of the repository. Make sure the repository is accessible from the McAfee ePO server.
Domain	Type the domain name.
User Name	Type the name of the user in the specified domain.
Password	Type the password to access the network location.
Test Connection	Click this to verify that you are able to connect to the repository with the specified credentials.
Add extracted certificates and installers to Rule Group	Select this option to add the extracted certificates and installers to a user-defined rule group.

Purge server task

Use this page to purge Solidcore reporting data. When you purge data, the records are permanently deleted.

Option definitions

Option	Definition
Choose Feature	Select the Solidcore reporting feature for to purge the records. • **Event** — Select this option to purge Solidcore events. • **Client Task Log** — Select this option to purge Solidcore Client Task logs. • **Alerts** — Select this option to purge Solidcore alerts. • **Inventory** — Select this option to purge inventory details for endpoints. • **Observations** — Select this option to purge observations generated for endpoints. • **Content Change Tracking Repository** — Select this option to purge content change tracking data. • **Image Deviation** — Select this option to purge image deviation details.
Purge records older than	Select this option to purge the entries older than the specified age. This option is not applicable for features that do not have ageing criteria, such as inventory records.
Purge by query	Select this option to purge the records for the selected feature that meet the query criteria. This option is only available for reporting features that support queries in McAfee ePO. Also, this option is supported only for tabular query results. NOTE: No seeded queries are available for purging. Prior to purging records, you must create the relevant query.

Run Image Deviation server task

Use this page to compare the inventory of one or more endpoints with the inventory of a designated gold system.

Option definitions

Option	Definition
Consider file paths as case-sensitive	Use this option to indicate whether to use case sensitivity for file paths while comparing the images. We recommend that you do not select this option for the Windows platform.
Gold System	Use this option to specify the gold system.
System to compare with Gold System	Add the endpoints to compare with the gold system.
Groups to compare with Gold System	Add system groups to compare with the gold system.
Include Systems with Tags	Add endpoints based on the specified tags to compare with the gold system.
Exclude Systems with Tags	Add endpoints based on the specified tags. The endpoints with the selected tags are excluded from comparison with the gold system.

Migration server task

The Migration server task runs automatically when you upgrade the Solidcore extension. Check the **Server Task Log** to ensure that migration was successful.

NOTE: If the migration fails, review the server task log, resolve any issues, and run the Migration server task manually to complete the migration.

Send Feedback to Application Control GTI Cloud Server server task

Use this page to configure and send feedback to McAfee on how you are currently using the GTI features.

Option definitions

Option	Definition
Policy Information	Use this option to send information on how you are using Change Control, Application Control, and General policies in your setup.
Event Information	Use this option to send event information for your setup. Selecting this option sends information, such as binary name and SHA1 value for the Execution Denied, Process Hijacked, and Nx Violation Detected events. • **System Information** — Use this option to send information on the number of endpoints on which the event occurred along with the full path of the binary file (for which the event occurred).
Inventory Information	Use this option to send inventory information for your setup. Selecting this option sends detailed information for binary files, including base name, embedded application name, embedded application version, embedded version, and so on. • **System Information** — Use this option to send information on the number of endpoints on which the binary file is present, its execution status, and full path of the binary. Note that the feedback does not include any information to identify the endpoints, such as system name or IP address.
ePO unique identifier	Use this option to send information on the unique McAfee ePO identifier for your setup.

Run Reconciliation server task

Use this page to run or schedule reconciliation for your setup.

NOTE: No additional configuration is required to run this server task.

General policy — Exception Rules (UNIX) page

Use this page to define rules to override or bypass the applied memory-protection techniques on the UNIX operating system.

Option definitions

Option	Definition
Add	Opens the **Add Attribute** dialog box. • **File** — Type the name of the file that you want to bypass from the applied memory-protection techniques. • **Process Context File Operations Bypass** — In certain scenarios, Application Control can prevent legitimate applications from running. Use this option to define a bypass rule for a file. Use this option judiciously because it may impact default Application Control functionality. • **Parent** — Use this option to specify the parent to allow the file to bypass the memory-protection feature (Process Context File Operations Bypass option) only if it is launched by the specified parent. • **OK** — Click this option to add the rule. • **Cancel** — Click this option to exit without saving the rule. NOTE: Contact McAfee Support for information on other deprecated memory-protection techniques, such as API Mangling, Decoying, and Virtual Address Space Randomization (VASR).
Edit	Opens the **Edit Attribute** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.

General policy — Exception Rules (Windows) page

Use this page to define rules to override or bypass the applied memory-protection techniques on the Microsoft Windows operating system.

Option definitions

Option	Definition
Add	Opens the **Add Attribute** dialog box. • **File** — Type the name of the file that you want to bypass from the applied memory-protection techniques. • **Bypassed from CASP (for Windows 32-bit)** — Use this option to bypass the selected file from the Critical Address Space Protection (CASP) technique. • **Bypassed from DEP (for Windows 64-bit)** — Use this option to bypass the selected file from the Data Execution Protection (DEP) technique. • **Bypassed from Call Context Verification (for Windows 64-bit)** — Use this option to bypass the selected file from the Call Context Verification technique. • **Bypassed from ASLR (for Windows 64-bit)** — Use this option to bypass the selected file from the Address Space Layout Randomization technique. • **Process Context File Operations Bypass** — In certain scenarios, Application Control can prevent legitimate applications from running. Use this option to define a bypass rule for a file on 32-bit and 64-bit Windows platforms. Use this option judiciously because it may impact default Application Control functionality. • **Parent** — Use this option to specify the parent to allow the file to bypass the memory-protection features if it is launched by the specified parent. This option is applicable only for the Process Context File Operations Bypass and Bypassed from ASLR options. • **OK** — Click this option to add the rule. • **Cancel** — Click this option to exit without saving the rule. NOTE: Contact McAfee Support for information on other deprecated memory-protection techniques, such as API Mangling, Decoying, and Virtual Address Space Randomization (VASR).
Edit	Opens the **Edit Attribute** dialog box with information for a selected rule. Edit the rule as required, then click **OK**.
Remove	Select this option to delete the selected rule.
Diagnostic Suggestions (relevant only for 5.1.5 or earlier versions)	Select this option to review available diagnostic recommendations. Use the suggestions to define rules to add updaters relevant for your setup.

General [Configuration (Client)] policy — CLI Settings tab

Use this page to change the default password for McAfee Solidcore Client CLI console access.

Option definitions

Option	Definition
Password	Type the password to access McAfee Solidcore Client CLI console.
Confirm Password	Confirm the new password.

General [Configuration (Client)] policy — Miscellaneous Settings tab

Use this page to configure the maximum file size for tracking content changes. By default, you can track changes for any file with a size of 1000 KB or lower.

Option definitions

Option	Definition
Maximum file size for Content Tracking	Type the maximum file size to track content changes.

General [Configuration (Client)] policy — Events Custom Message tab

Use this page to configure end-user notifications. The settings on this page determine if and the kind of customized notification message displayed on the endpoints for the various Application Control events.

Option definitions

Option	Definition
User Message	Use the **Show the messages dialog box when a event is detected and display the specified text in the message** option to display a message box at the endpoint each time a event is generated.
HelpDesk Information	Allows you to specify helpdesk information that is displayed on the endpoints. • **Mail To** — Type the email address to which all approval requests (from endpoints) are sent. • **Mail Subject** — Specify the subject of the email message sent for approval requests (from endpoints). • **Link to Website** — Indicates the website listed in the Application and Change Control Events window on the endpoints. • **ePO IP Address and Port** — Type the McAfee ePO server address and port.
Messages	Customize the messages displayed for the Execution Denied, File Write Denied, File Read Denied, Process Hijack Attempted, Nx Violation Detected, ActiveX Installation Prevented, and Package Modification Prevented events by using these options: • **Message** — Specifies the message text for the event. • **Insert Variable** — Allows you to add variables to notification message. • **Insert** — Click to add the selected variable to the message text. • **Show Event in Dialog** — Use this option to indicate if all events of the selected event type are listed in the Application and Change Control Events window on the endpoints.

Edit Permission Set — Solidcore Policy Permissions page

Use this page to define permissions for Solidcore policies while configuring permission sets.

Option definitions

Option	Definition
Solidcore 6.0.0: Application Control	• **No permissions** — Restricts users from viewing or modifying the Solidcore policy settings for Application Control. • **View settings** — Permits users to only view the Solidcore policy settings for Application Control configured by the administrator. • **View and change settings** — Permits users to view and modify the Solidcore policy settings for Application Control.
Solidcore 6.0.0: Change Control	• **No permissions** — Restricts users from viewing or modifying the Solidcore policy settings for Change Control. • **View settings** — Permits users to only view the Solidcore policy settings for Change Control configured by the administrator. • **View and change settings** — Permits users to view and modify the Solidcore policy settings for Change Control.
Solidcore 6.0.0: Integrity Monitor	• **No permissions** — Restricts users from viewing or modifying the Solidcore policy settings for Integrity Monitor. • **View settings** — Permits users to only view the Solidcore policy settings for Integrity Monitor configured by the administrator. • **View and change settings** — Permits users to view and modify the Solidcore policy settings for Integrity Monitor.
Solidcore 6.0.0: General	• **No permissions** — Restricts users from viewing or modifying the Solidcore General policy settings. • **View settings** — Permits users to only view the Solidcore General policy settings configured by the administrator. • **View and change settings** — Permits users to view and modify the Solidcore General policy settings.

Edit Permission Set — Solidcore General Permissions page

Use this page to define permissions for Solidcore features while configuring permission sets.

Option definitions

Option	Definition
Queries, Dashboards	• **No permissions** — Restricts users from running queries and viewing dashboards related to Solidcore. • **Run Queries, View Dashboards** — Permits user to run queries and view dashboards related to Solidcore.
Events	• **No permissions** — Restricts users from viewing Solidcore events. • **View Events** — Permits users to view Solidcore events. • **View Events, Manual Reconciliation** — Permits users to view and manually reconcile Solidcore events.
Responses	• **No permissions** — Restricts users from creating Solidcore event responses. • **Create Solidcore Event Response** — Permits user to create Solidcore event responses.
Alerts	• **No permissions** — Restricts users from viewing and dismissing Solidcore alerts. • **View Alerts** — Permits users to only view Solidcore alerts. • **View and Dismiss Alerts** — Permits users to view and dismiss Solidcore alerts.
Client Task Log	• **No permissions** — Restricts users from viewing and deleting Solidcore client task logs. • **View Client Task Log** — Permits users to only view Solidcore client task logs. • **View and Delete Client Task Log** — Permits users to view and delete Solidcore client task logs.
Reconciliation	• **No permissions** — Restrict users from viewing all reconciliation-related pages. • **Access to Reconciliation** — Permits users to view all reconciliation-related pages.
Inventory	• **No permissions** — Restricts users from accessing all inventory-related pages. • **Access to View Inventory** — Permits users to only view all inventory-related pages. • **Access to View, Modify, Import Inventory** — Permits users to view and manage inventory by using the inventory-related pages.
Solidcore Configuration	• **No permissions** — Restricts users from editing and running the Solidcore: Scan a Software Repository server task. • **Access to Repository Scanner** — Permits users to edit and run the Solidcore: Scan a Software Repository server task.
Observe Mode	• **No permissions** — Restricts users from viewing the Observations page. • **View Observations** — Permits users to view the Observations page.
Content change tracking	• **No permissions** — Restricts users from viewing the Content Change Tracking page. • **View Content changes** — Permits users to only view the Content Change Tracking page.

Option	Definition
	• **View Content changes, Set Base Version , Create Content Change Response** — Permits users to view and take actions from the Content Change Tracking page.

Installers tab

Use this page to define and manage installers for your setup.

Option definitions

Option	Definition
Actions	Specifies the actions that you can perform on installers. • **Add Installer** — Use this option to add an installer to your whitelist. • **Add to Rule Group** — Use this option to add an installer to a rule group. • **Check Assignments** — Use this option to view assignments for an installer. Installers can be assigned to policies and rule groups. • **Edit** — Use this option to edit the name of the selected installer. • **Remove** — Use this option to delete the selected installer. NOTE: The installers should be dissociated from rule groups and policies before deleting.
Search Installer	Allows you to search for an installer. • **Installer Name** — Use this option to search for an installer based on its name. • **Vendor** — Use this option to search for an installer based on the name of the vendor who published the installer. • **Search** — Use this option to search for installers based on the specified criteria.
Options	**Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the installers list.
Select all in this page	Use this option to select all the installers displayed on the current page.
Select all in all pages	Use this option to select all the installers displayed on all pages.

Publishers tab

Use this page to add and manage certificates or publishers for your setup.

Option definitions

Option	Definition
Actions	Specifies the actions that you can perform for the selected publishers. • **Add to Rule Group** — Use this option to add a certificate or publisher to a rule group. • **Check Assignments** — Use this option to view assignments for a publisher. Publishers can be assigned to policies and rule groups. • **Edit** — Use this option to edit the friendly name of the selected publisher. • **Extract Certificates** — Use this option to extract a certificate from a binary file. • **Remove** — Use this option to delete the selected certificate. • **Upload** — Use this option to upload a valid certificate.
Search Publisher	Allows you to search for a publisher. • **Issued to** — Use this option to search for a publisher based on the name of the organization which publishes the certificate. • **Issued by** — Use this option to search for a publisher based on the name of the signing authority. • **Extracted From** — Use this option to search for a publisher based on the path of the binary file from which the certificate was extracted. • **Friendly Name** — Use this option to search for a publisher based on the friendly name of the certificate. • **Search** — Use this option to search for a publisher based on the specified criteria.
Options	**Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the publishers list.
Select all in this page	Use this option to select all the publishers displayed on the current page.
Select all in all pages	Use this option to select all the publishers displayed on all pages.

Rule Groups tab

A default set of rule groups is included for Integrity Monitor and Application Control. Use this page to manage rule groups for Integrity Monitor, Change Control, and Application Control.

Option definitions

Option	Definition
Actions	Specifies the actions that you can perform on the selected rule group. • **Assignments** — Use this option to view policy assignment for a rule group. • **Edit** — Use this option to edit settings for the selected rule group. • **Delete** — Use this option to delete the selected rule group. • **Duplicate** — Use this option to duplicate the selected rule group. • **View** — Use this option to view settings for the selected rule group. (available on McAfee ePO 4.5 only)
Add Rule Group	Use this option to add new rule group.
Export	Use this option to export the required rule group(s) to an XML file.
Import	Use this option to import a rule group.
Filter	Allows you to filter the rule groups based on these criteria: • **Type** — Use this option to filter the rule groups by Solidcore feature (Application Control, Integrity Monitor, and Change Control). • **Platform** — Use this option to filter rule group by the operating system. • **Search** — Use this option to search for a rule group based on the configured criteria.
Options	**Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the rule group list.
Select all in this page	Use this option to select all the rule groups displayed on the current page.

Upload certificate page

Use this page to upload an existing certificate available to you.

Option definitions

Option	Definition
Select a PEM format certificate to import	Specifies the path of the certificate file to import.

Extract Certificate from Binary page

Use this page to extract certificates associated with one or more signed binary files present on a network share.

Option definitions

Option	Definition
Location	Type the path of the binary file. Make sure that the file path is accessible from the McAfee ePO server.
Domain	Type the domain name to access the network location.
User Name	Type the name of the user in the specified domain.
Password	Type the password to access the network location.

Add installer page

Use this page to add an existing installer to the McAfee ePO repository.

Option definitions

Option	Definition
Installer Name	Type the installer name.
Installer Path	Type the path of the installer.
Version	Specify the version for the installer.
Vendor	Specify the name of the vendor who published the installer.
Checksum(SHA1)	Type the checksum value for the installer.

Advanced File Comparison page

Use this page to compare any two files (or file versions) on an endpoint or on two different endpoints.

Option definitions

Option	Definition
File 1	Allows you to specify information for the file to compare. • **Group** — Use this option to select the group. • **Host** — Type the host name. • **File** — Type the name and path of the file. • **Version** — Select the version to compare.
File 2	Allows you to specify information for file for comparison. • **Group** — Use this option to select the group. • **Host** — Type the host name. • **File** — Type the name and path of the file. • **Version** — Select the version to compare.
Show Comparison	Click to compare the specified files. The files (attributes and content) are compared and differences are displayed.
Close	Click to return to the Content Change Tracking Files page.

File Versions page

Use this page to review the versions for a file for which you are tracking content changes.

Option definitions

Option	Definition
Filters	Filter the displayed information using these options: • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
Actions	• **View** — Open the **File Information** page that displays the contents and attributes for the selected version. • **Compare with previous** — Compares the selected version with the previous version and displays the differences in file contents and attributes. • **Compare with base** — Compares the selected version with the base version and displays the differences in file contents and attributes. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Compare Files** — Compares any two selected versions and displays differences between the file content and file attributes. • **Delete** — Removes the selected file versions from the McAfee ePO database. This does not alter or remove the actual file present on the endpoint. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the versions list. • **Set as base version** — Resets the selected version as the base version and deletes all previous versions (older than the new base version) of the file.

Content Change Tracking Files page

Use this page to view and manage all files for which content change tracking is enabled.

Option definitions

Option	Definition
Filters	Filter the displayed information using these options: • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
View versions	Click to view all versions for a file. The **File Versions** page lists all versions for the selected file.
Actions	• **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Delete** — Removes the selected file and all its versions from the McAfee ePO database. This does not alter or remove the actual file present on the endpoint. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the file list.

Solidcore Syslog Server — Details page

Use this page to add the syslog server as a registered server or edit settings for an existing syslog server.

Option definitions

Option	Definition
Syslog Server Address	Allows you to enter the server address. You can choose to specify the DNS name, IPV4 address, or IPv6 address.
Syslog Server Port	Allows you to modify the syslog server port (McAfee ePO 4.6 only). If you are using McAfee ePO 4.5, you cannot alter the port (default port (514) is used).
Syslog Facility	Specifies the type of logs the server will receive.
Send Test Syslog Message	Click to verify if the syslog server is reachable or not.

Application Control GTI Cloud Server — Details page

Use this page to edit seeded settings for the Application Control GTI Cloud server.

Option definitions

Option	Definition
Application Control GTI Cloud Server Address	Specifies the address for the GTI cloud server.
Server Certificate for Application Control GTI Cloud Server	Provides the path to the certificate for GTI cloud server.
Application Control GTI Cloud feedback Server Address	Specifies the address of the feedback server for the GTI cloud server.
Server Certificate of Application Control GTI Cloud feedback Server	Provides the path to the certificate for GTI cloud feedback server.
Test Connection	Click to verify the connection to the server.

Solidcore Integration Server — Details page

Use this page to add the integration server as a registered server to McAfee ePO or edit settings for an existing integration server.

Option definitions

Option	Definition
Integration server host name	Specifies the host name for the integration server.
Integration server port number	Specifies the port for the integration server.
Ticketing system host name/URL	Specifies the host name for the ticketing system.
Ticketing system user name	Specifies the user name for the ticketing system.
Ticketing system password	Allows you to specify the password for the ticketing system. • **Change password** — Use this option to change the specified password for the ticketing system • **New password** — Type the new password. • **Confirm the new password** — Confirm the new password.
Test connection	Click to verify that you are able to connect to the ticketing system with the specified credentials.

Allow or Ban Binaries wizard

Use this page to allow known binary or script files to run and prevent bad binary or script files from running. This page is displayed when you select the **Allow Binaries** or **Ban Binaries** action from these pages:

- **Inventory By Applications** page
- **Inventory Details** page (opens when you click **View Inventory** for an endpoint on the **Inventory By Systems** page)
- **Binary Details** page

Option definitions

Option	Definition

Allow Binaries	• **Add Binaries to Whitelist** — Use this option to add the selected binary files to whitelist of the endpoint. This option is available only when you open the wizard from the Inventory Details page.
	• **Add to Existing Rule Group** — Use this option to update an existing rule group with rules to allow the selected binary files.
	  • **Select a Rule Group** — Select the rule group to update.
	  • **Rule Group OS** — Specify the operating system for the rule group.
	• **Create a New Rule Group** — Use this option to create a new rule group with rules to allow the selected binary files.
	  • **New Rule Group Name** — Type the name for the rule group.
	  • **Rule Group OS** — Specify the operating system for the rule group.

Ban Binaries	• **Add to Existing Rule Group** — Use this option to update an existing rule group with rules to ban the selected binary files.
	  • **Select a Rule Group** — Select the rule group to update.
	  • **Rule Group OS** — Specify the operating system for the rule group.
	• **Create a New Rule Group** — Use this option to create a new rule group with rules to ban the selected binary files.
	  • **New Rule Group Name** — Type the name for the rule group.
	  • **Rule Group OS** — Specify the operating system for the rule group.

Observations page

Use this page to view the observations generated for the managed endpoints.

Option definitions

Option	Definition
Filter	Allows you to filter the displayed observations based on specified criteria, including: • **Time Filter** — Use this option to filter observations generated in the specified time period. • **Approval Status Filter** — Use this option to filter observations based on their approval status. • **Show Exclusion Rules** — Opens the **Solidcore Observation Exclusion Rules** page. Use this page to view and manage the defined exclusion rules.
Solidcore Observations	Lists all observations matching on the specified filter criteria. • **Hide Filter/Show Filter** — Use these to hide or show the filters in the pane. • **Quick find** — Use this option to specify the string to search for. • **Apply** — Click to filter the observations list based on the specified string. • **Clear** — Use this option to clear an applied filter. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page. • **Show Suggestions** — Opens the Observations Detail page that displays details for the observation.
Actions	• **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the Solidcore Observations pane. • **Delete Observations** — Removes the selected observations from the Observations page and the database. Select **Delete Similar Observations** to delete other related observations. All observations with the same checksum or file name on different hosts are considered similar observations. • **Dismiss Observations** — Ignores the selected observations (by setting their status to Dismissed). You can also choose to dismiss other related observations or define exclusion rules to stop receiving similar observations. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the observations list.

Observations Detail page

Use this page to analyze the suggestions available for an observation and take actions for the observation.

Option definitions

Option		Definition
Binary Tree		Allows you to review information for all the child observations associated with the opened collated observation. By default, the file associated with the collated observation is selected in this pane. The tree hierarchically represents the relationship between the file and its parent process. It also lists all the child observations generated for the file.
Suggestions tab	**Binary Info pane**	Displays detailed information for the selected binary file and lists all the actions you can perform for the file. Depending on the file's properties and attributes, one or more of the following actions are available for the file. • **Add as Installer** — Click to add the program (or installer) as an authorized installer for your setup. • **Add as Updater** — Click to add the program as an authorized updater for your setup. • **Add to Whitelist** — Click to add the file to the whitelist for a specific endpoint. Note that this action does not result in the any rule group or policy changes. • **Add Parent as Updater** — Click to add the parent program as an updater for your setup. • **Add as Exception** — Click to define a rule to allow the file to override or bypass the applied memory-protection techniques. • **Add by Checksum** — Click to authorize the program to run on endpoints based on its checksum value. • **Add as Trusted Directory** — Click to add the location for the file as a trusted directory for your setup. Note that the added trusted directory will be provided updater privileges.
	Publisher Info pane	Displays information for the certificate, if any, associated with the file. This pane is displayed only if a certificate is associated with the selected file. • **Add Publisher** — Click to add the certificate as a trusted publisher.
	Rule Group pane	Displays the various rules to be added to the rule group. By default, this pane is empty and is populated based on the actions you perform.
	Files to be Whitelisted pane	Displays the various files to be whitelisted on the endpoint. By default, this pane is empty and is populated only when you choose the **Add to Whitelist** action. • **Add** — Opens the **Add to whitelist** dialog box. Specify the binary path name. • **Remove** — Deletes the selected rule. • **Edit** — Opens the **Add to whitelist** dialog box with information for a selected rule. Edit the details as required, then click **OK**.

Option	Definition
Observations tab	Displays detailed information for observations in a tabular format.
Dismiss	Click to dismiss the observation.
Approve	Click to save the changes made and approve the observation.
Cancel	Click to exit without saving changes and return to the **Observations** page.

Solidcore Observation Exclusion Rules page

Use this page to view and manage the defined exclusion rules.

Option definitions

Option	Definition
Filter	Allows you to filter the exclusion rules based on specified criteria. • **Hide Filter/Show Filter** — Use these to hide or show the filters in the pane. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
Actions	• **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display in the page. • **Delete** — Removes the selected exclusion rule. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the exclusion rules list.
Close	Click to exit without saving changes and return to the **Observations** page.

Reconciliation Summary page

Reconciling changes generates a comprehensive list of the changes carried out on all managed endpoints, then groups and matches the changes with change tickets and approvals. Use this page to view reconciliation results.

Option definitions

Option	Definition
Reconciliation Summary	Provides a summary of the reconciliation results. • **Authorized Changes** — Displays the number of authorized changes made on all managed endpoints. Changes made as part of a change ticket are referred as authorized changes. • **Unauthorized Changes** — Displays the number of unauthorized changes made on all managed endpoints. Changes made without an associated ticket ID are referred as unauthorized changes. • **Changes that match multiple Tickets** — Displays the number of changes made on all managed endpoints that match multiple ticket IDs. • **Reconciled Tickets** — Displays the number of reconciled tickets (corresponding to which changes have been found) in your setup. • **Systems with Unauthorized Changes** — Displays the number of managed endpoints in your setup with unauthorized changes. • **Systems with Changes that match multiple Tickets** — Displays the number of endpoints in your setup with changes that match to multiple tickets.
Reconciliation Actions	• **Reconciliation Cycle Logs** — Opens the **Reconciliation Cycle Logs** page that lists the logs for all reconciliation cycles. The page includes one entry for each executed and in progress reconciliation cycle. • **Reconciled Tickets** — Opens the **Reconciled Tickets** page. Use this page to view the ticket IDs and reconciliation change details. • **Systems with Unauthorized Changes** — Opens the **Systems with unauthorized changes** page. Use this page to view the list of endpoints on which unauthorized changes were made and their change details. • **Systems with changes matching multiple Tickets** — Opens the **Systems with changes matching multiple tickets** page. Use this page to view the list of endpoints on which the changes made match multiple tickets.

Reconciliation Cycle Logs page

Use this page to view reconciliation logs. This page includes one entry for each executed and in progress reconciliation cycle. Click a record to review details for the cycle.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Preset** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page.
Actions	• **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the Reconciliation Cycle Logs page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the reconciliation logs list.

Reconciled Tickets page

Use this page to view the ticket IDs and reconciliation change details. Reconciled tickets are tickets that are associated with the appropriate events after reconciliation. The page includes one entry for each reconciled ticket.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Preset** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page.
Actions	• **View Changes** — Opens the **Authorized Changes** page. Use this option to view details for a particular ticket. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the this page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the reconciliation tickets list.

Authorized Changes page

Use this page to view all events matched with a particular ticket.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Filter** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page.
Actions	• **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the events list.

System with Unauthorized Changes page

Use this page to view the list of endpoints on which unauthorized changes were made and their change details.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Preset** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
Actions	• **Numeric link** — Opens the **Unauthorized Changes** page for the associated endpoint. Use this page to view all unauthorized events for the selected endpoint. • **Document Changes** — Opens the **Document Changes** dialog box that allows you to associate a ticket with all unauthorized changes for the endpoint. • **Dismiss Changes** — Opens the **Dismiss Changes** dialog box that allows you to ignore all unauthorized changes for the endpoint. Dismissed changes are removed from the page and not considered for future reconciliation cycles. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the endpoints list.

Unauthorized Changes page

Unauthorized change are events on the endpoints or groups that cannot be matched with any change tickets in the Change Management System. Use this page to view and manage unauthorized events for an endpoint.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Preset** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
Actions	• **Document Changes** — Opens the **Document Changes** dialog box that allows you to associate a ticket with the selected events. • **Dismiss Changes** — Opens the **Dismiss Changes** dialog box that allows you to ignore the selected events. Dismissed changes are removed from the page and not considered for future reconciliation cycles. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the endpoints list.

Systems with Changes matching multiple Tickets page

Use this page to view the list of endpoints on which the changes made match multiple tickets.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Preset** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
Actions	• **Numeric link** — Opens the **Changes that match multiple Tickets** page lists all unresolved events for the selected endpoint. • **Resolve changes** — Opens the **Resolve changes** dialog box that allows you to match all unresolved events for the selected the endpoint with a specified ticket. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the list of endpoints.

Changes that match multiple tickets page

Unresolved events are events that match multiple tickets in the change management system. Use this page to view and manage the unresolved events for an endpoint.

Option definitions

Option	Definition
Filters	Allows you to filter the listed details based on these criteria: • **Preset** — Use this option to review information for the specified time period. • **Hide Filter/Show Filter** — Use these to hide or show the filters on the page. • **Show selected rows** — Use this option to hide all rows except the rows selected on the page.
Actions	• **Resolve changes** — Opens the **Resolve changes** dialog box that allows you to match the selected unresolved events with a specified ticket. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the page. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the list of unresolved events.